DESIGNING, TESTING, AND USING COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, AND INTELLIGENCE (C4I) SYSTEMS: WHAT CAUSES THE DISCONNECTS AND WHAT CAN BE DONE ABOUT THEM?

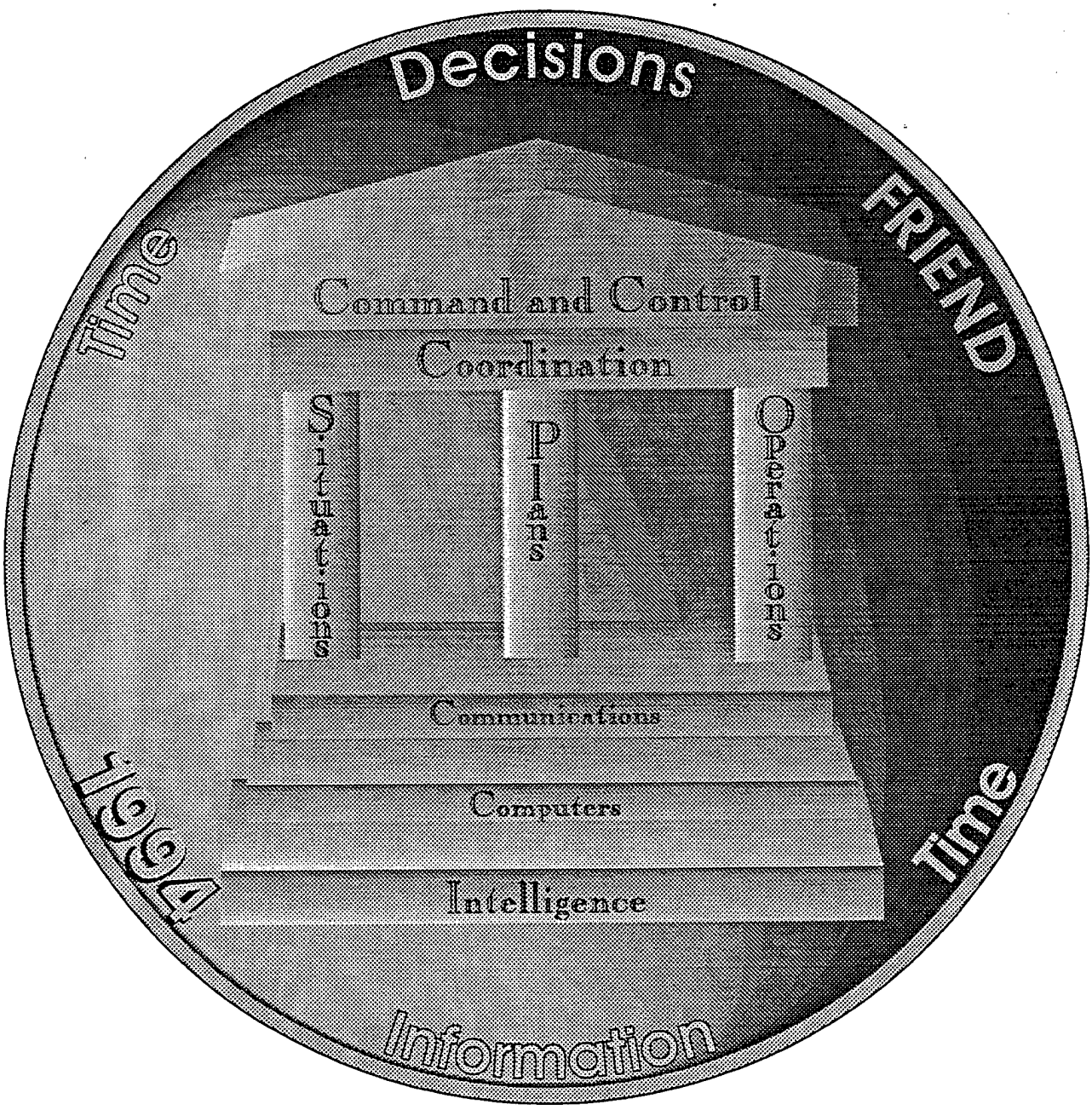
by

JAMES E. ARMSTRONG JR.
Lieutenant Colonel, United States Army

NAVAL WAR COLLEGE
Newport, Rhode Island

June 1994

Paper directed by
Captain Eugene K. Nielsen
Professor (Emeritus) Frank M. Snyder
Colonel Roger A. Ricketts


Decisions
FRIEND
time
Command and Control
Coordination
Situations
Plans
Operations
Communications
Computers
Intelligence
1994
Information
time

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	JUNE 1994	TECHNICAL REPORT

4. TITLE AND SUBTITLE
DESIGNING, TESTING, & USING COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, AND INTELLIGENCE (C4I) SYSTEMS; WHAT CAUSES THE DISCONNECTS & WHAT CAN BE DONE ABOUT THEM.

5. FUNDING NUMBERS

6. AUTHOR(S)

LTC JAMES E. ARMSTRONG, JR.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMA OPERATIONS RESEARCH CENTER
WEST POINT, NEW YORK 10996-1779

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A.
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

THE PURPOSE OF THIS WORK IS TO IDENTIFY AND EXAMINE THE DISCONNECTS IN DESIGNING, TESTING, AND USING COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE (C4I) SYSTEMS, INVESTIGATE THEIR CAUSES AND EFFECTS, AND DETERMINE WHAT CAN BE DONE ABOUT THEM. TO ACCOMPLISH THESE PURPOSES, EXPERTS INVOLVED WITH RESEARCHING AND ANALYZING, DESIGNING AND DEVELOPING, TESTING AND EVALUATING, AND MANAGING, OPERATING, AND USING C4I SYSTEMS OFFERED THEIR THOUGHTS ON THE SUBJECT IN STRUCTURED INTERVIEWS. THESE EXPERTS REPRESENTED THE MILITARY, ACADEMIC, AND COMMERCIAL C4I COMMUNITIES INCLUDING THE DEPARTMENT OF DEFENSE, THE JOINT STAFF, AND THE ARMY, NAVY, AND AIR FORCE STAFFS. IN THIS WORK, THE EXPERTS' OPINIONS BLENDED WELL WITH A REVIEW OF THE LITERATURE.

14. SUBJECT TERMS	15. NUMBER OF PAGES
C4I	139
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	

EXECUTIVE SUMMARY

The purpose of this work is to identify and examine the disconnects in designing, testing, and using Command, Control, Communications, and Intelligence (C4I) Systems, investigate their causes and effects, and determine what can be done about them. To accomplish these purposes, experts involved with researching and analyzing, designing and developing, testing and evaluating, and managing, operating, and using C4I systems offered their thoughts on the subject in structured interviews. These experts represented the military, academic, and commercial C4I communities including the Department of Defense, the Joint Staff, and the Army, Navy, and Air Force Staffs. In this work, the experts' opinions blended well with a review of the literature.

In no way does this effort attempt to catalog every problem related to C4I systems. Instead, the intent is to identify the main, overriding issues that dominate current thinking about C4I systems. Therefore, this descriptive research depends, in part, for its success on the Pareto principle: although there are many problems, most of the serious difficulties are due to just a few of them. Hopefully, the selective sample of experts and the literature review has successfully identified some of the serious problems and explored some ways to begin to resolve them.

The research discovered eighteen major disconnects which are listed in the conclusions and discussed throughout the text. First, many difficulties stem from the rapid advances in the underlying information technologies. Although the Department of Defense (DOD) used to

drive these advances, they are now clearly driven by the commercial, non-defense sector. DOD, the Joint Staff, and the Services have a number of promising initiatives underway. Resolving this disconnect requires two important ingredients. First, a *process* needs to be established and continually improved to *determine and manage change*. Part of this process must have *mechanisms to get inside the commercial development world of information technology* or DOD will increasingly "be on the outside looking in."

Complicating the first disconnect is the burdensome and lengthy acquisition process. This disconnect makes C4I systems more costly than needed and often the systems are quickly out-of-date, old and undesirable, especially when compared to the commercial world. These *legacy systems* are difficult to use and maintain. Efforts to migrate legacy systems need to be accomplished. However, no "one time fix to the problem" will suffice. Since all systems progress through a lifecycle, they will all, at some point, need to be retired or evolved into a new system. Hence, every system may, at some point, become a legacy system or require a plan to evolve it to a new one. Again, a *process to continually manage legacy systems* is needed. Reforms to the acquisition process are also needed. Reforms that embrace *incremental, evolutionary development* and allow for *a closer partnership between DOD and the commercial sector* are overdue.

Historically, the Services have developed separate "stovepipe" systems for command and operations centers, communications systems , and intelligence systems. Difficulties with interoperating these "stovepipe" systems in a joint warfare environment are well known. The Joint Staff addresses this disconnect by requiring interoperability certification, compatibility testing, standards compliance, and security accreditation. Although these initiatives are very

helpful, they tend to be a symptomatic treatment. A *"system of systems"* approach headed by a senior warfighter needs to replace the hold that the communications and intelligence communities have on C4I. With the blurring between the strategic, operational, and tactical levels of warfare and the blurring between peacetime and conflict, it is time for a holistic approach to C4I.

Within each service, there are many functional areas that all have legitimate C4I needs. Still these needs must be addressed in an integrated, disciplined way. This disconnect can cause the same information to get collected twice or not to be available to those with a legitimate need. Each service must have a "system of systems" approach to C4I that coordinates across functional areas within a service and across warfare areas with other services. Again, a senior warfighter is the right leader for shaping a service's C4I systems. Although the communications and intelligence specialties have much to contribute to C4I systems, the systems need to focus on the warfighter.

The definition of successful design is meeting the effective needs of the user. In C4I systems, users are the commanders and warfighters. This means the front-end of the design process, specifying user requirements, is very important. Unfortunately, because of the meager resources applied to the requirements end, user requirements lag technology and are unstable and ill-defined. As a result, systems are fielded that do not meet the effective needs of the user. Systems engineers, representing the user, need to provide an interface between the warfighter and the detailed design engineers to ensure that valid requirements are generated. Designs of C4I systems must be trusted to those who understand systems engineering methodologies and processes. A common understanding of C4I architecture

needs to be spread through the C4I community. Promising methods are available now for understanding and modeling the functional, physical, and operational architecture of C4I systems. The services must take advantage of this technology so they can analyze the performance of architectures before any networks and nodes are installed and operated.

The final and perhaps most tragic disconnect in design is that there is no consistent approach to automation and human-machine interaction for C4I systems. The result is often the unintentional loss of human life during operations due to fratricide or other unintentional errors. Information technology and human-machine systems design research offers many promising approaches. An understanding of the human, process, and system interactions and error modes must be achieved and worked in interactive, virtual environments before C4I systems are actually built and deployed.

Testing and evaluation of C4I systems suffer from a lack of metrics and an ad hoc approach to system integration. As a result, it is difficult to evaluate the value-added of investments in C4I systems. Also, existing systems remain in operation beyond their useful life because they are rarely re-evaluated. Systems are not robust and are difficult to maintain once the "ad hoc integrators" that put the project together move on to another contract. Resolving these difficulties requires that legacy integrators be replaced by true systems integrators. Importantly, rapid prototyping of C4I systems with a "build a little, test a little" approach is desirable. Testing should focus on functionality and usability. Can the system do what the user wants it to do and is it easy for the user to get the system to do it?

Many disconnects filter down to the user. As mentioned, systems often lack true functionality. They simply cannot do what the user wants and needs them to do. Sometimes,

even though the functionality is there, the systems are too difficult to operate. The user interfaces often do not support thinking in warfighter terms. The result is that users sometimes revert to manual procedures and find systems less useful than they could be. Better designs and testing will overcome some of these obstacles. Usability centers that involve real users in simulated operational environments can correct many of these problems. Most importantly, C4I systems must be adaptable to the operational realities of the users' warfare environments.

As C4I system building progresses and information technology advances, there are strong implications for changes to the command and control process and warfare itself. C2 organizations will become flatter as levels of hierarchy are eliminated because many routine recordkeeping and bookkeeping tasks have been automated and consolidated in higher echelons.

Situation assessment may be quicker and better and involve less human effort. Why? Because artificial barriers to information collection and dissemination will be removed. Distance will become meaningless in a communications sense since advances in communications technology may make every node in a C4I system seem equidistant. Thus information will be routinely available everywhere. Moreover, the compilation of all this information into an understandable situation picture will be enhanced by information fusion, display, and multi-media technologies. This will give warfighters the ability to recognize and understand situations much earlier in the time window of opportunity -- from when a situation develops until the opportunity for action disappears.

The paper discusses many more aspects of how the C2 process and warfare will change. Warfare has always had main three aspects: maneuver, firepower, and information. What continues to change in warfare is not the basic nature of warfare but instead the technological advances that make it possible to make more advances in one aspect or another of warfare. The US Armed Forces have been effected by three main revolutions in warfare: firepower warfare when advances in technology such as rifled artillery and the machinegun gave great advantages to firepower and resulted in the trench warfare of World War I; manuever warfare when technology such as the internal combustion engine, the tank and aircraft linked by radio made possible the "blitzkreig" of World War II; and now we are in the midst of information warfare where the many advances in information technologies have greatly increased the ability to gather, process, store, display, and transmit information. This does not mean that firepower and manuever are no longer important. It does mean that the preponderance of technological advances that offer new opportunities for improving military effectiveness are information-based.

In other words, it is the means to carry out warfare that changes not its basic nature. If the underlying nature of warfare was truly changing then the study of the history of warfare would be sheer folly. We know that many valuable lessons about warfare can be learned from history. And as some have pointed out, one thing we learn is that nations in the past have taken different approaches to how best to take advantage of new technologies for the conduct of war. The winners are those armed forces that develop appropriate operational concepts and make the organizational changes necessary to get the maximum military effectiveness from new technologies in military systems.

There are several important questions from a command and control perspective. First, are the military forces or operations that commanders and warfighters control going to be so different that changes in the C2 process or C4I systems need to be considered? Is the nature of modern warfare operations changing so significantly that we need to adjust doctrine, force structure, operations, and training?

Information technologies, stand-off weapons platforms, precision guided munitions, and smart missiles will blur the distinction between the strategic, operational, and tactical levels of war mainly because communications technologies and stand-off weapons will increasingly make every location on the globe seem equidistant from every other location. Also blurred will be the distinction between peace and war since the opportunities and vulnerabilities for engaging opponents with information technology resources will be so lucrative or so potentially damaging that constant vigilance will be required to serve and protect the nation. Information technologies provide opportunities to engage an adversary's information resources, manage the perceptions of their leaders, confuse their population, and mislead their armed forces. However, the globalization of information technologies makes all nations potentially subject to these vulnerabilities. Although a distinction may be drawn between information-based warfare, which may be ongoing at all times, and command and control warfare (C2W), which tries to destroy and disrupt enemy C2 capabilities while protecting friendly C2, both will be ongoing continuously. Only the decision making authority and the scope of the operations will distinguish them. As a result, systems to monitor and control information resources and C4I systems are needed.

Even though the basic nature of warfare may not change in terms of the basic objectives of war, the means to accomplish war, the number of functions that a commander must coordinate and the number of different types of weapon systems involved, continue to be more complex. Doctrine needs to accommodate these changes and emphasize winning the information war. Force structures need to account for the increased importance of the information dimension of warfare. Organizations and staffs should be able to be made flatter and smaller respectively by using information technology to accomplish many routine and burdensome tasks. Training and education need to integrate formal classes on command-and -control and C4I systems. This does not mean that warriors need to be immersed in technical C4I knowledge or jargon. Instead, commanders and warfighters need an operational knowledge of C4I systems with an understanding of how people, the command and control process, and C4I systems work together to win information operations, prosecute C2 warfare, and accomplish command and control. But winning requires more than knowledge as Sun Tzu warns, "One may *know* how to conquer without being able to *do* it."

ACKNOWLEDGMENTS

I want to thank the people who made this research effort possible. First, many thanks to the faculty at the Naval War College that supported this work especially Captain Eugene K. Nielsen, Professor (Emeritus) Frank M. Snyder, and Colonel Roger A. Ricketts. Without their enthusiastic support and encouragement, this project would never have been possible. Also, the hard work of Professor John B. Hattendorf and Lieutenant Commander Joseph T. Dunigan was especially helpful. They do a very admirable job in making the Advanced Research Department a creative and stimulating research environment.

Several organizations deserve special mention. The MITRE Washington C3 Center, thanks to Charles Hall, was very helpful in sharing their valuable experiences and professional knowledge. The Center for Excellence in C3I at the School of Information Technology and Engineering, George Mason University, donated their time and expertise. My thanks to Dean Andrew P. Sage and Professor and Director of the Center, Harry Van Trees, for making the visit and interviews at their school so useful. I also want to thank the Director of the Operations Research Center at the United States Military Academy and Professor and Head of the Systems Engineering Department, Colonel James L. Kays, for supporting a good part of this research.

Importantly, a special thanks to the many hard working military officers and civilian officials who took time out of their busy schedules to be interviewed for this work. And, to my family for their patience and understanding while the effort was ongoing.

TABLE OF CONTENTS

C4I SUBSYSTEMS AND LESSONS FROM THE PERSIAN GULF

INFORMATION TECHNOLOGY TRENDS

INITIATIVES AND ACQUISITION STRATEGIES

CONCLUSIONS AND RECOMMENDATIONS

CHAPTER I

INTRODUCTION

On April 14, 1994, a sunny, clear day in southern Iraq, two US Army Black Hawk helicopters carrying 15 Americans, 3 Turkish officers, 2 British officers, and one French officer were on a mission to monitor the protection of Kurdish refugees in northern Iraq. The team of officials were surprised to see two American fighter planes streak by their flight path. Minutes later, radar and missile warning receivers started screaming and lit up the front control panels of both Black Hawks. Frantically, the helicopter pilots started trying to communicate with the Airborne Warning and Control System (AWACS) aircraft in the area and double checked that their Identification Friend or Foe (IFF) system, which automatically transmits friendly identification signals to other aircraft, was working. Seconds later, two missiles, launched from the same two US F-15C jet fighters that had patrolled past them earlier, slammed into the Blackhawks, shredding the helicopters into pieces and killing all twenty-six people on board.[1]

One month earlier, a C-130 had just been cleared for take-off from Pope Air Force Base at Ft Bragg, North Carolina. The crew of five people had just started lifting the aircraft into the clear blue sky on their way to complete a routine transport mission. As they lifted off the runway, they saw a C-141 loading up with soldiers from the 82nd Airborne Division. They could see the soldiers talking and working to check equipment on their buddies jump

---

[1] Michael R. Gordon, "26 Killed as U.S. Warplanes Down Two US. Helicopters Over Kurdish Area of Iraq," *New York Times*, 15 April 1994, 1.

harnesses as the soldiers were loading into the aircraft and getting ready for the daily practice parachute jump. Seconds later, as they turned their attention again to the blue skies, they were startled to see a flash and then felt a tremendous jolt as an F-16 fighter swooped into their flight path, colliding with them and tearing off a piece of their fuselage. As the pilot of the Hercules C-130 transport worked feverishly to control the plane and turn it back to the runway, he was terrified to see the F-16 jet tumble toward the ground and crash into the fuselage of the C-141 Starlifter loaded with soldiers. Instantly the C-141 burst into flames and the tragic scene unfolding on the ground underneath them was to kill 23 soldiers and injure 100 more.

Five months before the Ft. Bragg mishap, Task Force Ranger, made up of some of America's most highly trained forces, Delta commandos and US Army Rangers, set out in Mogadishu, Somalia by helicopter and "humvees" to surround and capture the Somali warlord Mohammed Farah Aideed and his top lieutenants. Although the first 15 minutes of the operation were highly successful due to the capture of 25 of Aideed's top aides, what was supposed to be a quick operation soon turned into a massive firefight with thousands of Somalis. The combat lasted through the night, into the next morning and left 18 American soldiers killed, 84 more wounded, and 1 captured alive and displayed on CNN (Cable News Network), Chief Warrant Officer Michael J. Durant. Aideed lost more than 1000 of his forces and the capture of many of his top lieutenants. Still, the brutal scenes of Americans being dragged through the streets of Mogadishu by the native peoples that they had gone there to feed were shocking. Those images probably helped convince President Clinton to withdraw all US forces from the chaotic country by the end of March 1994. The account of the

operation is filled with details of the confusion and carnage suffered by US forces and the difficult decisions made under fire at every level of command.[2]

Other incidents give testimony to the fact that command and control in modern warfare is a difficult, and sometimes deadly business. In 1988, the USS Vincennes misidentified a civilian Iranian airliner, shot it down and unintentionally killed 290 people. What makes command and control so difficult for modern commanders? One observer points out,

> It is the very ambiguity of the political and military contexts in which contemporary fighting men are asked to operate, and the speed with which advanced technology sometimes forces them to make decisions, that troubles many who have pondered modern warfare. Planes move so fast, and weapons are so lethal, that judgments must often be almost instantaneous and mistakes often exact a far greater toll.[3]

Technology has long been looked at as the answer to many modern warfare dilemmas. Why is it becoming a problem now? According to some analysts, technology makes mistakes more likely today because it is overwhelming human beings' abilities to control the forces under their command. "It is not that people do stupid or careless things. Modern technology has simply evolved so fast and in so many different ways that it is overtaxing human capacities, and that makes it far more difficult to prevent these things," concludes one military analyst.[4] Speaking about the accidental shoot down of two American Black Hawk helicopters over Iraq, Defense Secretary William Perry said that "there were human errors, probably, and there might be process or system errors as well."[5]

---

2 Rick Atkinson. "The Raid That Went Wrong: How an Elite U.S. Force Failed in Somalia," *The Washington Post*, 30 January 1994, Sunday, Final Edition, 1-20.

3 R. W. Apple Jr., "Trigger Fingers: Has Technology Made Mishaps More Likely?," *New York Times*, 15 April 1994, 1.

4 Ibid.

5 Ibid.

What do American warfighters have to help them make these important decisions about positioning and operating forces and weapons in difficult and dangerous situations? C4I (Command, Control, Communications, Computers, and Intelligence) systems is, of course, the answer. But, as these tragic incidents demonstrate, that answer is not yet right. Apparently, there are a number of difficulties or disconnects that cause C4I systems to fall short of our expectations about them. The purpose of this research is to examine the disconnects in designing, testing, and using C4I systems, investigate their causes and effects, and determine what can be done about them.

This focus on C4I systems does not mean that the human dimension of command and control is discounted. Far from it. Instead, this work takes the perspective that a system is a group of parts or components that work together for a specified purpose. Since people are an integral part of C4I systems, working with computers and communication devices and links to support the command and control decision making process of military commanders and warfighters, understanding their role inside, and interaction with, C4I systems is crucial. However, any reasonable approach for developing trustworthy C4I systems must recognize that roles for people in these systems must be designed within the human beings abilities for successfully carrying out the tasks allocated to them. Therefore, issues that describe the difficulties that people experience with C4I systems are also part of this research effort. Further, this research explores possible changes to command and control processes and to warfare in terms of doctrine, force structure, operations, and training implied by removing or mitigating C4I disconnects and thereby taking full advantage of information age technologies.

To accomplish these purposes, this research interviewed twenty experts associated

with researching, analyzing, designing and developing, testing and evaluating, and using C4I systems. In addition to structured interviews with experts representing the academic, military, and commercial research communities, the Department of Defense to include the Joint Staff J-6, and the Army, Navy, and Air Force Staffs, review of related literary efforts are included.

Defining the Disconnects

Defining the disconnects requires an understanding of several related processes. The first process relates to information technologies which form the basis for the communication links and devices, computer hardware and software, and the intelligence sensors and processors that make-up C4I systems. The commercial market, not DOD, drives the information technology process which produces a new generation of products and services every one and one-half years.

The second process is the DOD acquisition process where military users define requirements and then select primarily civilian designers and developers to produce concepts and prototypes which are tested and then selected for full-scale production and fielding. The acquisition process, often criticized for burdensome bureaucratic delays, takes from six to nine years from system definition to actual system deployment. Hence during one acquisition cycle, information technology moves through four to six generations of development.

Making the situation worse is the fact that user requirements often lag even current technology. Therefore, the relatively lengthy acquisition cycle may start its long process already a generation behind. The result of this disconnect is that C4I systems are fielded with obsolete technology that fails to satisfy a user's "command and control" needs. If a new C4I system is successful in incorporating truly innovative technology, a frequent result is that the

new system does not integrate well with existing systems. But there are disconnects that go beyond this simple picture because of the way we have historically put C4I systems together.

As Frank Snyder points out, we do not design and build C4I systems. Instead we separately design and test three different systems: telecommunications systems, intelligence systems, and command centers.[6] The commanders and military users in the field are largely left to form these three separate systems into a coherent, working whole.[7] But this "stovepipe approach" does not stop there.[8] Instead, it is compounded by the separate development process of each of the services. That means that the Army, Navy, and Air Force each have their own parallel process for separately developing their own communication systems, intelligence systems, and military operations centers. The result of this disconnect is that C4I systems are fielded by the services that do not interoperate in the joint warfare environment. But even within a "stovepipe", a single, functional system within one service, there are difficulties in designing, testing, and using these systems. Chapter II examines the main issues and their associated causes and effects that cause difficulties in designing C4I systems.

Another disconnect is the gap that exists between designers and testers. The testing community is frequently hard pressed to understand the C4I system under evaluation because that community has no clear understanding of the systems design architecture and no standard architecture to use as a basis for comparison.[9] Often testers try to apply weapon system

---

[6] Frank M. Snyder, interview by author, written notes, Naval War College, Newport, Rhode Island, 26 April 1994.

[7] The Defense Information Systems Agency (DISA) and the Headquarters of the respective Armed Services have many integration efforts ongoing. Some of these are discussed in Chapter VII.

[8] A stovepipe, a tall, closed vertical pipe, has come to represent a narrow-minded approach for designing and developing a subsystem chiefly from the point of view of a single function without due regard for how the subsystem relates to other subsystems, or for how the subsystem contributes to the larger operation of the whole C4I system.

[9] Although the Defense Information Systems Agency has a Center for Standards, it does not appear that there is concrete, usable knowledge about how to evaluate a proposed C4I system to determine if it

testing paradigms to the evaluation of C4I systems.[10] Since there is not yet a universally accepted theory of command and control, testers find it very difficult to develop metrics of C4I systems that can relate C4I system performance to combat effectiveness. Chapter III examines the main issues and their associated causes and effects that cause difficulties in testing C4I systems.

In summary, all of these disconnects add up to two main problems plaguing C4I systems. First, C4I systems are not really designed and tested. Instead, separate communication systems, command and operations centers, and intelligence systems are fielded by the services and it is largely left up to the commander in the operating forces, to put these systems together into a workable, coherent C4I system. Chapter IV discusses some of the user perspectives on C4I systems.

Second, making this situation worse, is that military commanders are not prepared to do this "field assembly" very well because they and their subordinates are not educated or trained to understand the command and control process, the C4I systems supporting that process, nor the underlying information technologies. Instead, commanders are given lots of operational experience in the hope that by this exposure they will learn all they need to know about command and control. Although most military officers are quick to say that their main purpose in war is to command and control their assigned forces, none of the military educational institutions have military command and control as a required course. In fact, one of the interesting findings from the interviews was that many of the experts thought that very

---

satisfies DISA's standard architecture.

[10] An example weapon system testing paradigm is to test a unit without the new weapon and compare that unit's effectiveness with a similar unit using the new weapon. The main measure of effectiveness for these simple comparisons is kills of enemy systems or loss exchange ratios. Since C4I systems do not kill anything in a direct sense, such weapon system testing paradigms applied to testing of C4I systems are fraught with many difficulties.

few designers, testers, or military users of C4I systems had an adequate understanding of command and control. This research supports the view that significantly more educational efforts are needed to broaden and deepen the understanding of the military command and control process and supporting C4I systems.

Command and Control

Explaining what command and control means in this research is essential for several reasons. First, there has been much confusion about the many terms and acronyms associated with command and control (C2). For example, what is the difference between C2 and C4I? Military commanders often differentiate between the two words. They consider command as the art and practice of making important decisions about how to position and operate military forces. They consider control to be the science of carrying out staff work to support and execute the commander's decisions.[11] Others refer to command as the legal authority vested in certain military positions.

In this work, command and control (C2) refers to the human decision making that takes place to position and operate military forces. The longer acronyms, such as C4I, refers to a system, a group of components, people, procedures, communication devices and links, computers, and intelligence assets, that work together to help accomplish command and control. Terms like C4I emphasize the activities and technologies that enable command and control: communications, computers, and intelligence. Often people will attach a new letter to the C2 acronym to highlight a particular supporting activity or technology. Chapter V discusses some of the difficulties associated with the various subsystems and components of

---

[11] D. Shoffner, "Future Battlefield Dynamics and Complexities Require Timely and Relevant Information," *PHALANX*, (March 1993): 1.

C4I systems. The main point to remember is that the enabling activities and technologies are all subordinate to and support the central purpose of command and control, decision making. What then is the nature of decision making in military command and control?

Decision making in command and control situations is distributed. Distributed decision making involves a well-trained team, which is typically geographically dispersed. Information about the team's situation is also distributed across the team members. No one person has a complete picture or even the same view of the entire situation.[12] Decision makers in command and control situations must consider how their decisions will impact the rest of their team. They must monitor not only their own predicament, but they must also have some appreciation for the status of their teammates. This means that C2 decision makers need information that is appropriate for their role in the team. But, they also need information about the rest of their team so they can make better decisions and take coordinated actions. Hence, coordination is a basic requirement of any C2 system.[13]

C2 decision making is driven by combinations of events called "situations." A situation[14] is a combination of events that creates an opportunity for decision making and

---

[12] Even though it might be technically possible to give every person the same information with the same level of detail, it would not be humanly possible for people to process the information because people have a fundamental limit to the amount of information they can process especially in time-constrained situations. Because of these limits on human information processing, echeloned teams of commanders coordinate to command and control military forces. In the Navy, the Anti-Surface Warfare Commander concentrates on a different set of information than the Anti-Air Warfare Commander. However, they must work together to use their limited resources to protect the Carrier Battle Group. In the Army, the Corps Commander has a summarized, aggregated set of information about battalions compared to the detailed information available to a Battalion Commander.

[13] Coordination is the ability to combine military forces in synchronized action so that the forces, working or acting together, have a greater overall effect than otherwise. As in any team situation, although coordination can and should be planned in advance, it is very dependent on events and thus usually requires the exchange of information under the stress of combat operations.

[14] Situations are events as they actually happen, not events as they may be perceived by the commander. One important objective of a C4I system is to help the commander accurately assess the situation and reduce the discrepancy between the commander's perceptions and reality.

subsequent action. Situations give meaning and worth to decisions and actions. To determine if an appropriate decision was made requires an understanding of the context of the situation. Situations change with time. They arise and expire. This means that there is a time window-of-opportunity associated with every situation -- the time from when a situation first develops until the time when the opportunity for action disappears. To be effective, a commander must be able to recognize and understand a situation soon enough in the the time window-of-opportunity so that relevant planning and combat operations can take place before the time window-of-opportunity closes. Situations can occur simultaneously or sequentially. The time sequence of arrival of situations affects the difficulty of the decision making. Time is a critical consideration and making decisions requires information. Therefore, the value of information in C2 is very sensitive to time.

Because time is so critical in the C2 *process*, helping commanders with the recognition and response to the development of situations is the main purpose of C4I *systems*. C4I systems help the commander accomplish this main purpose in three ways: recognizing and understanding *situations*; formulating and disseminating *plans*; and directing and monitoring combat *operations*. This does not mean that the command and control process needs to be reactive. Successful commanders, according to DePuy, often anticipate situations and have a dominating concept of the operation[15], a mental construct of how they will shape the current and future situation to achieve their desired objectives. However, the situational view does recognize that the command and control process is two-sided. There is an enemy commander trying to carry out a similar process. Therefore, the successful commander must always be

---

[15] William E. DePuy, "Concepts of Operation: The Heart of Command, The Tool of Doctrine," *Army Magazine*, August 1988, 26.

alert to enemy capabilities, intentions, and actions that might necessitate the execution of a branch or sequel of the original plan or a transition to a new plan. Making these kinds of judgments, such as evaluating the cost of changing to a new scheme of operations versus staying with the original concept, is one example of the difficult decisions that need to be supported by C4I systems.

The command and control process is enabled by the activities and technologies of communications, computers, and intelligence. Intelligence is the means for creating information from data gathered from many sources. Communications are the means for transferring information which enables decision making as well as the directives and orders that result from decision making. Computer are support tools embedded throughout the process. Note that the entire structure depends on a base of information. Assessing the situation, developing plans, and carrying-out operations requires making decisions based on accurate, timely information. Intelligence is the means for creating this all-important information. It is no surprise then to appreciate the importance of information technology to command and control. Chapter VI discusses trends in information technology, lessons learned from the Persian Gulf Conflict, and examines their relationship to future C4I systems.

DOD, the Joint Staff, and the Armed Services have recognized the challenge and opportunity that getting C2 right represents and have invested considerable effort in developing acquisition strategies to cope with some of the disconnects. Chapter VII reviews the acquisition strategies and initiatives of the services and explores their potential for eliminating or mitigating the existing disconnects. Chapter VIII summarizes the standard practices, emerging principles, and promising future directions identified by this research that

can contribute to designing and fielding better C4I systems and conducting more effective combat operations. The purpose of this effort is not to identify every issue associated with C4I systems. That would be an impossible task. Rather, the intent is to identify the main issues that seem to be dominating the concerns of the US military as they work to leverage information age technologies for the common defense.

CHAPTER II

DESIGN

Three issues dominated both the interview responses and the literature reviewed. These issues concerned requirements, architecture, and standards. A fourth issue, automation, emerged from the literature review. Although the services have recognized the need to address these issues and have some promising initiatives underway, a concern with some of their logic is the focus on a fixed set of discrete solutions. The pace of changes sweeping through the underlying technology base for information products and services is compelling evidence that the answer to getting C4I systems right lies in establishing a process that can cope with change. The solutions identified today must be constantly reviewed by a process that can evaluate current solutions in light of technological advances. The age of fixed solutions that can last for any period of time is gone.

Requirements

Ideally, the acquisition process begins in earnest when military users, spurred by the identification of operational needs, write a set of requirements for a C4I system. This means that the requirements define the system that is eventually developed and deployed. Hence, specifying requirements correctly is probably the most important part of the design process.

Unfortunately, despite the importance of user requirements, there are several major problems that make it difficult to write useful requirements for C4I systems. First, users often lack the requisite knowledge of operational needs and of the state of technology to produce

useful requirements. Although there are users with expert knowledge about operational needs, they are not usually the ones tasked to write requirements. Requirements writing is often accomplished by relatively junior personnel with inadequate senior officer involvement. Second, requirements suffer from the "stove pipe" tunnel vision perspective of the user communities and services and lack specific information on integration and interoperability. Further requirements are often ill-defined and unstable, subject to unpredictable change during the development process as explained later.

There are two types of knowledge that seem to be most valuable when writing requirements: operational knowledge and technical knowledge. Operational knowledge is the knowledge that users have gained from years of experience with actually operating in a warfighting environment and using C4I systems. Technical knowledge is an appreciation for what can be achieved with the underlying technologies that make C4I systems work. For C4I systems, this means an understanding of the capabilities and possibilities of information technology. Requirements need to reflect both types of knowledge. The best requirements would reflect not only a combination of what is operationally needed with what is technically possible to achieve but also might be a careful statement of a warfare need that calls for the application of technology in ways never before tried. In other words, requirments writers need to be innovative. Unfortunately, very few users have an adequate knowledge of where technology is headed. Often the user is tied to the operational constructs of existing systems and is unable to adequately express requirements in terms of functionality, not to mention, new operational concepts or tactical innovations.

Once the system definition process begins, users learn more about what is technically possible. As a result, requirements tend to change with the user now orienting on a specific technical solution instead of new ways of meeting operational needs. Unfortunately, some of these technical solutions are not really that new since designers and developers tend to focus on solutions that are well known to them as well. Therefore, users tend to state requirements in obsolete terms.

To bridge this gap, users need help in writing requirements and designers need to gain a solid appreciation for the operational environment. System engineers who specialize in requirements engineering are essential to the process. For example, requirements engineers know that requirements should be written in a hierarchical manner so that designers and testers understand how requirements relate to each other. Also, the user needs "technology scouts" with user experience as part of the process to overcome both user and designer fixations with old solutions. These technology scouts would spend time in the commercial sector learning about promising trends and concepts that might have application to the user's mission or functional area.

The other problem with requirements is that the user normally suffers from "tunnel vision" when writing requirements. This means they consider only how a new system will meet their own functional needs and they fail to consider how a new system will interact with other functional areas. Since the users normally have a difficult enough time writing requirements for their own functional area, it is easy to understand why requirements often fail to adequately address integration and interoperability needs with other functional areas. A way to bridge this gap is to create multi-functional user teams or multi-functional reviews of

requirements. Another way to overcome some of these difficulties is to develop a coherent architecture that can guide the development efforts of all C4I systems.

Architecture

The main problem with architecture and C4I systems is twofold. First, few people, both uniformed and civilian, understand what architecture means in terms of C4I systems. Second, there is not yet a well-known, accepted standard architecture for C4I systems.[16] Architecture, in general, is a scheme of arrangement or plan. The plan typically consists of common identifiable parts and explains or depicts their *relation* to each other. The way these parts fit and work together as a whole determine the character or style of the architecture of the system. The architecture of a system also explains how the parts of the system conform to basic principles. Frank Snyder defines system architecture to include three aspects. The identification of the system's subsystems, the allocation of the subfunctions that the system must perform to subsystems, and the standards for interfaces between subsystems.[17]

Researchers at the Center for Excellence in C3I at George Mason University's School of Information Technology and Engineering define C3 architecture at three levels: functional, physical, and operational.[18] The functional architecture describes the various functions that the system must do and how the functions relate to each other. The physical architecture specifies the physical entities that comprise the system and details on which entities the

---

16 The DOD Technical Reference Model for Information Management published in May 1992 does establish a generic architecture and standards profile for DOD-wide compliance. What remains to be seen is how service components will transition existing systems into compliance with the standards profile and how successful they will be in tailoring the reference model to a specific mission area and using the reference model as a basis for designing new systems. Although every system now functioning has an architecture, the problem is that these architectures are not well articulated and understood.

17 Frank M. Snyder, *Command and Control: The Literature and Commentaries*, (Washington D.C.: National Defense University Press, 1993), 132.

18 Lee W. Wagenhals, interview by author, written notes, 6 April 1994, Center for Excellence in Command, Control, and Communications and Intelligence, George Mason University, Fairfax, Virginia.

functions reside. The operational architecture allocates tasks to the physical architecture and establishes rules of operation for all functions. This means the operational architecture describes how the various entities work together during all modes of operation. This operational description is very important since once it is known, the system can be modeled and tested on a computer before it is actually built and placed into operation.[19] The other great advantage of this approach to C4I system architecture is that the systems engineer can

> translate between user requirements, functional requirements and system performance... [and can] Maintain a consistency between multiple models of the same system:..maintenance of consistency provides the audit trail and the translator link between the user (who determines the requirements) and the executable model that provides the analysis of performance. The effort required, while substantial, is proving to be worthwhile.[20]

Walter R. Beam stresses the importance of creating an evolvable C3 system architecture. He says, "Good system architecture anticipates likely directions of system and technological evolution and adapts readily to new system requirements and technology as they come along."[21] To accomplish this end, particular attention must be paid to the architectural details of system interfaces. These interfaces include interactions among the system components, with users, with other systems and with the operational environment. For example, Beam suggests adopting national or international standards for interfaces when they are suitable for a system. In the computer arena, such practices broaden the present and future options for hardware and software. Importantly, Beam recognizes that this will not always be possible and that existing standards may need to be extended or new ones devised. Further, he emphasizes that even if interface standards are selected that can survive

---

[19] Dennis M. Buede, Didier M. Perdu, Lee W. Wagenhals, "Modeling the Functionality of the C2 Element of the National Missile Defense System," in *Proceedings of the Symposium on Command and Control Research June 28-29, 1993*, (Washington, D.C.: National Defense University, 1994), 246.

[20] Ibid., 255.

[21] Walter R. Beam, *Command, Control and Communications Systems Engineering*, (New York: McGraw Hill, 1989), 161.

technological advances for a reasonable system lifetime, the point may be reached when the system can no longer communicate effectively with newer systems. At this point, the old system may be technically obsolete and may need to be replaced and standard interfaces evaluated and updated. Beam suggests the following design principle to guide system architects,

> Never unintentionally inhibit expansion upward, downward, laterally, or functionally. The good architect assumes that the highest hierarchic level of the system will some day be an intermediate level of a larger or more advanced system. Likewise, the lowest level in the initial design will be required to support lower-level subsystems. Lateral expansion will require ability to address, at any level, larger numbers of subsystems than initially contemplated.[22]

Standards

From a commercial perspective, standards are "Specifications for hardware and software that is either widely used and accepted (de facto) or is sanctioned by a standards organization (de jure)."[23] Since standards are an important part of the architecture of a C4I system, some thoughts on how to evaluate standards for adoption are in order. Andrew P. Sage discusses the role of standards in systems engineering efforts and makes several key observations.[24] First, using standards represents a trade-off between innovation and integration. Without standards, many useful systems as we know them simply would not be possible because their parts would not fit or work well together. Still, adherence to a rigid standard stifles the ability to cope with dynamic environments. Hence, standards should be carefully considered and should not be used when a more flexible guideline would be sufficient. Sage points out that while standards are a minimum acceptable requirement,

---

22 Walter R. Beam, *Command, Control and Communications Systems Engineering*, (New York: McGraw Hill, 1989), 162.

23 Alan Freedman, *Electronic Computer Glossary*, 1993.

24 Andrew P. Sage, *Systems Engineering*, (New York: John Wiley, 1992), 162-7.

guidelines are only suggestions and provide for greater flexibility and judgment. Alan Freedman emphasizes,

> Standards is the most important issue in the computer field...very few standards...are universally used. This subject is as heated as politics and religion to vendors and industry planners...The standards makers are always trying to cast a standard in concrete, while the innovators are trying to create a new one. Even when standards are created, they are violated as soon as a new feature is added by the vendor. If a format or language is used extensively and others copy it, it becomes a de facto standard and may become as widely used as official standards from ANSI [American National Standards Institute] and IEEE [Institute of Electrical and Electronics Engineers]. When de facto standards are sanctioned by these organizations, they become stable, at least, for a while. In order to truly understand this industry, it is essential to understand the categories for which standards are created [machine languages, data codes, hardware interfaces, storage media, operating systems, and communications, programming languages, file management systems, text systems, and graphics systems].[25]

In one person's view, the standards challenge is to adopt standards that "embrace the future and allow for expandability far more than they currently do."[26] For the C4I community, the challenge is to apply standards in a way that provides for current interoperability, without inhibiting effective systems in the future.

Sage says that standards should be kept up to date and that the costs and benefits of following a standard or not following it should be well understood. This implies that standards should not be blindly perpetuated. Rather, standards should be rigorously challenged and replaced when new standards are more cost-effective or when simple guidelines become more practicable. For example, the Ada[27] software standard for DOD may

---

25 Alan Freedman, *Electronic Computer Glossary*, 1993.

26 Ibid.

27 Ada is a high-level, Pascal-based programming language developed by the US Department of Defense. A programming language is used by computer programmers to write instructions, software code, for the computer. Pascal , also a high-level programming language and named after the French mathematician, Blaise Pascal, was developed in the 1970s by Niklaus Wirth, a Swiss professor. A high-level programming language can translate into one or more machine instructions whereas a low-level language needs one statement for every machine instruction. Ada is named after the world's first documented computer programmer, Augusta Ada Byron who lived from 1815 to 1852. Countess of Lovelace and daughter of Lord

be a case in point. Developers of software contend that the Ada standard triples the cost of all DOD software contracts. If this is so, then DOD should be required to show the benefit they are receiving exceeds the additional cost. For example, consider the fact that by 1995, the DOD will spend 42 billion dollars on software alone.[28] If the Ada standard represents two thirds of that cost, then the Ada standard may be costing DOD 28 billion dollars each year! DOD could build several new aircraft carriers each year or buy an Air Force wing or pay the entire operations and maintenance budget for the Army with those savings.

Proponents of maintaining the Ada standard often offer the comparison of Ada versus "spaghetti code."[29] They also have maintained that the Ada standard makes software code purchased by DOD re-usable but there is much evidence that very little code has been re-used.[30] Further, evidence suggests that there is much commercial off-the-shelf code[31] that could be inexpensively used by DOD but DOD is not permitted to use it without first paying to have the code translated to Ada. Finally, without question, there are a number of sophisticated programming languages for software that are viable alternatives to Ada such as the commercial de facto standard of C.

Byron the English poet, she was a mathematician and worked with a British scientist, Charles Babbage, to help develop the first programmable calculator. See Alan Freedman, Electronic Computer Glossary, 1993.

[28] General Accounting Office, *Test and Evaluation: DOD Has Been Slow In Improving Testing of Software-Intensive Systems*, Report no. NSIAD-93-198, (Washington, D.C.: U.S. Government Printing Office, 29 September 1993.

[29] Spaghetti code is contrasted with structured code or programming languages that have embedded techniques that enforce a logical structure on the writing of a program. In reality, all programming languages are structured; however, some have more structure than others. Languages with less structure rely more on the discipline of the programmer to make the logic of their programs easy to follow and test. Spaghetti code has usually referred to programming languages such as BASIC that have many "GO TO" statements which cause great difficulty for readers of the program to understand the program's flow of logic.

[30] General Accounting Office, *Software Reuse: Major Issues Need to Be Resolved Before Benefits Can Be Achieved*, January 28, 1993, Report no. IMTEC-93-16.

[31] The de facto standard language for developing commercial software is C. Working at Bell Labs in the 1980s, Ken Thompson and Dennis Ritchie developed C as a way to port the computer operating system they invented, UNIX, to other machines. Because C is very flexible and can compile into machine language for almost any computer, C has become the programming language of choice in the commercial world.

Therefore, intelligent evaluation of existing and future standards is needed. Sage also says that unenforceable standards[32] and those that impose a specific solution should be avoided. Again using the Ada example, perhaps a conceptual software standard that outlines the various beneficial features of Ada may be an alternative to the implementation standard of Ada.

One of the most frequent solutions offered to solve many of the difficulties associated with building C4I systems is a standard, open architecture. What does this mean and why do many people think this approach will work? In its most general sense, open means that "an end user should be independent of any particular vendor."[33] For example, an open system would have software that can be easily ported from one platform, type of computer hardware, to another. Another aspect of an open system is that their technology is publicly accessible to developers. As one industry expert says, "This is good for hardware and operating system vendors because it promotes a software industry that generates value added products designed to run on their products. This is good for me because I don't need to generate zillions of different versions of my code designed to run in different environments."[34]

So what is open architecture? Open architecture[35], from a computer perspective, is a system design that is compatible with hardware and software from many vendors of many product families.[36] The technical specifications of open systems are made public to promote

---

32 One example of an unenforceable standard is where authorities grant so many exceptions to the standard that the standard is no longer meaningful.

33 Peter Collinson, "Open Doors," *EXE*, February 1994, 36.

34 Ibid.

35 An open system, as defined here, is probably never completely achievable. Innovation will likely make some product families incompatible with others. However, from a C4I systems perspective, it should be possible to achieve a large measure of openness by specifications that define the interfaces among the applications, the application platforms, the operating system services, and the external environment.

36 Harry Newton, *Newton's Telecom Dictionary*, May 1994.

and encourage competition.[37] Hence, a standard open architecture would be an open design that is widely accepted and used. Sage says, "The term open systems architecture is now used to describe any of several generic approaches the intent of which is to produce open systems that are inherently interoperable and connectable without the need for retrofit and redesign."[38]

What are the prospects for success with a standard open architecture? Some cite the Apple II's early success as an example of open architecture. Many third party software vendors developed add-on products for the Apple II because Apple shared some of their technical specifications and even provided a set of software development tools for the Apple II in order to encourage third-party vendors to develop Apple II software applications. The IBM PC was also an example of open architecture from a software perspective. Also, the many "clones" that developed from the IBM PC are evidence that it is also somewhat open from a hardware perspective. But software could not be used across the two hardware types, Apple and the PC. The mainframe computer and later, the workstation computer, evolved with similar difficulties. Eventually, the goal of open architecture is to have software applications that are independent from the hardware and the operating system.

Automation

The allocation of functions among humans and machines is a traditional systems engineering design consideration. What has made this traditional question even more important today is the tremendously improved capabilities available now and in the future for automating many human decision making tasks.

---

37 Alan Freedman, *Electronic Computer Glossary*, 1993.

38 Andrew P. Sage, *Systems Engineering*, (New York: John Wiley, 1992), 168.

The main issue is how much automatic or computer control versus manual or human control should be designed into modern C4I systems. As Arnett says, "at issue is the degree to which machines will make and carry out battle decisions independent of their human counterparts."[39] Arnett contends that computers will be required to do more and more filtering and sifting of data, since the increased pace of modern war with the huge amounts of data gathered would overwhelm human decision makers. Therefore, he argues that machines in the form of computers would eventually have to dominate decision making on the modern battlefield. This new concept is often termed "cyberwar" where robots and unmanned platforms such as cruise missiles do more of the killing, making pilots and other human control roles on platforms of war obsolete.

It is interesting to compare this vision of warfare to current practices both in industry and war. For example, in factory settings, humans are no longer manual controllers of machines, instead humans are often in indirect or *supervisory control* of machines. This means that many routine decisions are accomplished by machines with the human intervening only to help resolve unforeseen ambiguities that were anticipated in advance. In the Gulf War, although AWACS and JSTARS controllers vectored pilots to advantageous attack positions, most final engagement decisions were human controlled.

Three control modes are possible for people in modern systems: manual, supervisory, and automatic. Manual control involves people providing the physical and intellectual impetus to decide what the system will do and where it will do it. Automatic control involves people programming a machine in advance to accomplish certain tasks when it receives certain inputs.

---

[39] Eric H. Arnett. "Welcome to Hyperwar." *The Bulletin of the Atomic Scientists* 48, no. 1, (September 1992): 15.

There are advantages and disadvantages to both of these modes of control. Manual controllers are constrained by human information processing limits and human physical abilities. Automatic controllers are constrained by the tasks and environmental situations envisaged by their creators. Fortunately, human supervisory control is a way to have the best of both manual and automatic control. In supervisory control, people accomplish higher-level cognitive tasks for which they are well suited such as planning and decision making in novel situations. Machines are delegated all physically arduous tasks and routine decision making tasks such as recordkeeping. Decision making tasks that have a high cost involved with making a wrong decision can be handled by a combination of human and machine. For example, the computer can nominate a target for destruction based on pre-programmed criteria but the human can retain ultimate "trigger authority".

The advantages of supervisory control as the standard mode of control for warfare are enormous. First, the effect of each human is multiplied through the indirect manipulation of multiple machines. For example, a pilot, instead of controlling just one aircraft with one set of weapons, could in a supervisory control mode, be responsible for multiple air platforms. Based on a given mission, the pilot could script the flight patterns in advance and change them on-the-fly as targets were found and engaged. If the manned "mother" craft was shot down, the unmanned "children" could be adopted by other nearby manned platforms. Although these possibilities are not easy to accomplish, they should not be ignored just because they are challenging.

An even more futuristic concept would be using a remote pilot situated in a virtual reality based on the actual situation being encountered by his multiple aircraft. The pilot

would still have all of the advantages of intimate familiarity with the context of the battle situation since he would be in the thick of the virtual fight yet protected from exposure to enemy air defenses.[40] Higher level human controllers above the pilot would be working on coordinating the current and future efforts of similar formations. Other controllers, applying the lessons being learned from similar, concurrent operations, would be making software adjustments that could be sent to the formations for on-line updates to improve the tactics, techniques and procedures employed by the supervised aircraft.

As timelines for tactical decision making decrease and the need for accuracy increases, it is possible that the human may often not be directly in the decision loop. Instead, people will indirectly control the decision making rules that machines use to function during these nearly instantaneous tactical engagements. But, it is important that military commanders have a C4I system that will let them know when these pre-programmed techniques, tactics, and procedures are not working well. Further, commanders will need a quick way to make the necessary changes across the forces. For example, it is not far fetched to imagine in the future that a C4I system will detect that a missile is being successfully decoyed by an enemy. The C4I system might assess the situation and determine that an adjustment to the missile software code is necessary. Over telecommunication assets the software fix would be tested in virtual simulations in the US and deployed into theater across the force to every missile's code within hours or even minutes.

This view of automation does not imply that people are less important than machines in warfare. Rather it implies that people need to be allocated C4I tasks that make the most of

---

[40] The sensor systems that provide the data to create the virtual reality world would probably be exposed to damage and deception.

their capabilities and take into account their limitations. Machines should be tasked to carry out tasks for which they are better suited and to support the enhancement of human capabilities and the amelioration of human limitations. Returning to the tragic examples of C4I failures discussed earlier, the fratricide of two US Blackhawk helicopters and the unintentional shootdown of a civilian airliner, there are three possible sources of error: the *human*, the *process*, or the *system*. In C4I systems, it is crucial that the designer has a thorough understanding of how each of these three elements can go wrong and how they interact with each other in the intended operational environment.

CHAPTER III

TEST AND EVALUATION

Evaluation is a process which should begin during the early design stages of a system and continue throughout the life of a system. The main purpose of the evaluation process is to judge whether or not the system satisfies the effective needs of the user in an efficient way. Tests are events in the evaluation process that seek to answer specific questions that will inform judgments about how and whether or not to procure, field, and retire a system. The evalution process determines the degree of excellence of a system's characteristics, those features that delinieate it as a C4I system and those features that may distinguish it from other C4I systems. Also, the evaluation process determines how the attainment of those features combine to accomplish the main purposes for which the C4I system was designed. This part of the evaluation process also considers whether or not there are better ways or better systems that could accomplish the same purposes. Also, the evaluation process examines whether the purposes the system serves are still needed.

C4I systems are tested to assure system quality. From a user perspective, quality is a description of the various characteristics of a system and the grade of excellence of those characteristics, plus an understanding for how the levels of achievement of these characteristics help the system attain its purposes. For example, some characteristics or attributes of a C4I system are reliability, interoperability, and usability. Sage describes quality as "the degree to which the attributes of the operational system enable it to perform its

specified end-item functions so as to achieve client purposes in acquiring the system."[41] The primary means of assuring quality in a system is testing. According to Sage, there are three different perspectives for conducting tests: structural, functional, and purposeful.[42] Structural testing examines the hardware and software details of systems such as the performance of an individual microchip or the reliability of a section of software code. Functional testing examines the input-output performance of the system to determine if the technical specifications are met. Purposeful testing determines if the system really does what the client wanted it to do. Five issues dominated the interview responses and the literature reviewed on testing and evaluating C4I systems. These concerns were degradation in interoperability, evaluation of legacy systems, measurement of C4I systems, value-price trade-off judgments, and time and resources for testing.

Interoperability

When systems, units, or forces can exchange services and information directly and can easily use the exchanged services and information to better operate together, then the systems, units, or forces are interoperable. This definition leads to two types of interoperability, procedural and technical. Procedural interoperability relates to the exchange of services such as establishing standard operating procedures and vocabulary for providing fire support or early warning information. Technical interoperability relates to the direct exchange of information and services usually among communications-electronics systems and items of equipment. Technical interoperability depends on technical issues such as standard message formats, protocols, and "whether or not radio equipment at each end is capable of transmitting

---

41 Andrew P. Sage, *Systems Engineering*, (New York: John Wiley 1992), 132.

42 Ibid., 135.

or receiving electrical signals with a common wave form, a capability that can be achieved using different hardware so long as signal interface standards have been established and observed."[43]

As Frank Snyder points out, ever since the Grenada operation in 1983, the Secretary of Defense and the Joint Staff have been very interested in achieving interoperability for C4I systems. In fact, they have gone so far as to require that all C4I systems are considered to be for joint use and therefore all are subject to meeting interoperability requirements.[44] These strict interoperability requirements have focused a lot of the testing efforts on determining if C4I systems are truly interoperable. If directives, policies, and instructions have required C4I systems to be interoperable more than 10 years ago then why is their such unanimous concern among the C4I community that it is still a big issue?

There are several reasons why achieving interoperability is still a big challenge. Perhaps the biggest cause of the difficulty has been the degradation in interoperability that a system experiences during the acquisition process. Apparently, most interoperability reviews and audits were focused on the early part of a C4I system's lifecycle, primarily on the system requirements. As the system evolved through its development process, often system technical specifications and actual delivered systems achieved a level of interoperability below the stated requirements. One way interoperability is degraded is that a system may be planned to interoperate with other new systems that never get fielded due to budget cuts. Another way is that budget cuts to a program may cause features in the new system that provide

---

[43] Frank M. Snyder, *Command and Control: The Literature and Commentaries*, (Washington, D.C.: National Defense University, September 1993), 111.

[44] Department of Defense Directive 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems*, November 12, 1992.

interoperability to be cut. To correct this gap between interoperability requirements and actual "deliverables," the Joint Staff has now required more interoperability reviews throughout a C4I system's acquisition process.[45] Formerly, systems in the later stages of development were not scrutinized for interoperability. Now, C4I systems will be checked for interoperability at several stages in their development. This interoperability review should probably be extended to apply to C4I systems throughout their lifecycle. For example, when C4I systems are modified or improved, they should have to pass an interoperability review.

Another problem that has degraded interoperability is the way we fund and field C4I systems. C4I systems are not funded as a large program or "system of systems". Instead we fund many relatively small programs and therefore field many separate components of the entire C4I system at different times. Therefore what looks very interoperable on paper, may due to budget cuts and program delays, may not in fact interoperate when actually deployed because the "family of C4I systems" that was envisioned to exist is missing partial or ven complete generations. This has led to a problem that is very strongly related to the interoperability issue: legacy systems.

Legacy Systems

Because we want the latest technology in our C4I systems[46] and because C4I systems are really comprised of many smaller programs spread across the services and spread across various functional proponents within the services, existing systems increasingly do not work well with the newer systems. These older systems are known as legacy systems. Generally,

---

[45] Chairman of the Joint Chiefs of Staff Instruction 6212.01, "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems," 30 July 1993.

[46] Wanting to use the latest technology for technology's sake alone may not be desirable. According to Frank Snyder, to the extent that this view becomes a "driver," using the latest technology (or wanting to), instead of trying to satisfy warfare requirements may be a large disconnect.

legacy has referred to the huge database information systems that exist on older mainframe computer systems which are hard to use and expensive to maintain. But legacy has come to have a wider meaning which is "any aging or disagreeable system, regardless of the technology.[47] In fact, some say, "The computer industry is saturated with legacy systems, legacy development software, legacy hardware, and even legacy vendors."[48] Defense Secretary William Perry, in an effort to improve interoperability and reduce costs, asked the Defense Information Systems Agency (DISA) to consolidate systems and applications by identifying interim standard information systems. Although this is a much needed effort, it is, as one industry analyst describes it, a monumental job. For example,

> DISA's Center for Integration and Interoperability has identified about 21,000 legacy applications or stovepipe systems across the Defense Department. But that figure is based on rough estimates and covers only command-and-control systems and intelligence systems.[49]

This problem of accumulating a large number of expensive information systems over time and trying to sort out which ones are needed and which ones to replace or upgrade is not unique to the Armed Forces. The commercial sector is experiencing a similar phenomena that is a rapidly growing problem. It is estimated that legacy systems that must migrate or die represent a multi-billion dollar problem for industry for years to come. In fact, in the commercial marketplace, because of the many products that are being designed to integrate legacy systems with newer systems, there is evidence that industry believes legacy systems will always be a fact of life. For example, in Microsoft's new Chicago operating system architecture, their "Plug and Play" feature, which permits the operating system to

---

[47] Paul Winsburg, "What About Legacy Systems?," *Database Programming & Design* 7, no. 3, (March 1994), 23.

[48] Robin Bloor, Changing of the Guard: Moving to Client/Server Environments May Mean Updating Your Legacy Staff," *DBMS* 7, no. 4, (April 1994), 12.

[49] Joyce Endoso, "Pentagon Brass Behind Schedule in Nominating Standard Systems," *Government Computer News*, 7 February 1994, 3.

automatically adjust the system configuration when new devices are added or when existing devices are removed, incorporates the ability to accommodate many legacy devices.[50]

What are the problems with legacy systems? A 1993 survey of 400 corporate information officers in the US and Canada say that legacy systems "do not provide enough access to management information, are difficult to maintain and enhance, and are unresponsive to business needs."[51] The answer to these problems, according to many, are open, client/server-oriented systems.[52] In a client/server system, "Each individual (and computer) operates independently and yet, when required, gathers [acts as a client for] or delivers [acts as a server of] ideas and information to others."[53] A great advantage of the client/server model is the tremendous reductions in network traffic that are possible.

The major problem with legacy systems now is how to evaluate them. Which legacy systems should migrate and which one should be eliminated? This is a major issue in DOD. Currently, only a set of guidelines has been established to accomplish the evaluation of legacy systems. Some of the analysis is at the ABND level (Analysis by Name and Description). If the system has a name or description that duplicates a newer system, then it is a candidate for elimination. Costs to eliminate and costs to keep the legacy system are also part of the analysis. More details of the policies for legacy systems are in Chapter VII.

Integration

The seamless self-configuration ideas in "Plug and Play" are worthy goals but will not be achieved for some time into the future. Therefore, making new systems work well with

---

50 Jeff Prosise. "Under Construction: Plug and Play," *PC Magazine*, 12 April 1994, 204.

51 Rachel Parker. "Better Access. Development Time Sell Client/Server," *InfoWorld*, 18 April 1994, 74.

52 Ibid.

53 John K. Piraino. "Preparing for the 21st Century: Client/Server More Than a Technology, It is a Management Philosophy." *DBMS* 6. no. 13. (December 1993), 10.

existing systems and possible future systems, integration, will continue to be a very important part of any C4I system development effort. Many companies advertise themselves as system integrators. The military often speaks of the commander as an integrator. If there is so much expertise in integration, what is it really and why is it often cited as a problem? First, system integrators generally do not produce systems of hardware and software. Instead, they assemble the products and services of others into a complete system. To do this requires lots of testing to ensure that the components selected for integration, such as a new application, routine, or electronic device, works well with the existing system. If the integration effort is successful in putting a new or improved system smoothly into operation without problems, then it is a seamless integration. A transparent integration means "that there is no discernible change after installation." from the user's viewpoint.[54] Hence, it is important to realize that much of the testing that C4I systems undergo, especially early in the development process, will be performed by a systems integration contractor.

The problems with systems integrators are several. First, the term systems integrator came to be associated with someone who installs and maintains a computing operation.[55] Historically, the people who accomplished this work had no educational background in systems engineering processes or methodologies. What they did have was an ability to put computer technology together and to make it work. Unfortunately, it was often accomplished in an ad hoc fashion. As a result, the installations of these systems were not very robust. Successful operation of these ad hoc systems depended on key people, lots of organizational memory, and expensive vendor support. Even minor modifications to these hand-crafted

---

54 Alan Freedman, *Electronic Computer Glossary*, 1993.

55 Ibid.

systems were costly. Since these systems were crafted and not engineered, they did not provide for expansion and growth. Fortunately, there are a number of prestigious educational institutions that offer programs of study in systems engineering to meet this critical need in today's information-based society. Still, it will take time for these educated professionals to mature with hands-on experience, rise through the corporate ranks and replace the "legacy integrators."

The other problem with systems integrators besides education is that often times they become advocates of particular products or vendors. This can happen due to financial incentives or it can happen because it is easier to work with familiar products than to exert the effort to keep abreast of new products and services. For this reason, some believe it is very important for DOD to maintain a competency in systems integration.[56] Paul Strassman writes,

> DOD must be the master integrator of contractors. While reliance on contractors is essential for most system projects, DOD must safeguard the interoperability of systems and the sharing of software assets. The excessive costs and redundancies of present DOD systems are largely caused by letting each integrator integrate their own contract. Consequently, DOD owns thousands of non-interoperable applications that are obstacles to rapid joint warfare. DOD capabilities to direct, architect and manage systems integration must be one of the core war fighting competencies of US forces, especially for information intensive warfare.[57]

Integration is a crucial concern from a testing perspective because, if integration is going to be accomplished successfully, then testing must be accomplished incrementally. First, testing is needed to make sure individual components of C4I systems meet their stated specifications. Next, testing should be conducted to make sure the components work together successfully as a system in a way that satisfies the warfighter's functionality and usability

---

[56] Paul Strassman wrote the letter to the editor of Government Computer News in response to an article which reported that LTG(retired) Paige, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, had decided to out-source or contract the service and reverse Strassman's decision for DOD to become its own integrator, when he had Paige's job.

[57] Paul A. Strassman, Letters to the Editor, *Government Computer News*, 16 August 1993, 30-32.

requirements. That is, does the system do what the user needs it to do and is it easy for the user to operate. Finally, testing must prove that the system, when placed into operation, will work well with existing and future systems. A popular way to phrase this need for incremental testing is, "build a little, test a little."

Measurement

A major difficulty that arises in testing C4I systems is deciding what to measure and interpreting what the metrics mean in terms of the contribution of the proposed C4I system to overall force effectiveness. Generally, the C4I community has described a hierarchy of measures to help guide testing efforts. At the lowest level, measures of performance (MOPs) determine how well the individual C4I system performs its assigned functions. Measures of effectiveness (MOEs), the next higher level, determine how much better the overall C4I system performs as a result of the new individual C4I system. At the next and usually the highest level, measures of force effectiveness (MOFEs) determine the increase in overall effectiveness as a result of fighting the force with the improved C4I system. Unfortunately, MOFEs have historically not shown very significant increases in effectiveness due to better C4I systems. Often it is even difficult to show that the overall C4I system is performing significantly better due to some new and improved C4I equipment. To overcome this difficulty, some researchers have argued for measures of merit (MOMs) that can be used to describe the overall benefit derived from improving a C4I system.

The main cause of this difficulty, and the way to resolve it, lies in the nature and purpose of C4I systems. C4I systems are, by their basic nature, decision making systems that process, store, transfer, use and display information. The purpose of these decision systems is

to support military decision making for positioning and operating military forces. The expectation then of providing better support to the decision making process is that better decisions will result which will cause forces to operate better and hence achieve better results. Historically, testers have focused too much on information flow and assumed that more information flowing means improved command and control. Unfortunately, such an approach ignores the problem of information overload which can make command and control worse. It also fails to discriminate, prioritize, or value the information provided. Just having access to information does not guarantee its timely or effective use and does nothing to make it relevant to potential decisions. The reason for using the information flow approach is that it is easy to measure and allows testers to ignore the complicated intervening command and control process and battle dynamics that obscure the effects of improved C4I equipments and systems.

There are several promising approaches for solving this dilemma. The first approach is to recognize the process of providing information, making decisions, and conducting battle. As outlined to a Military Operations Research Society Mini-Symposium on Measures of Effectiveness for C3, there is a four step methodology that could be applied to any scenario.[58] First, operational commanders wargame a scenario to determine for a particular concept of operation, what decisions need to be made and what information they require to support those decisions. Second, C4I experts should deploy the new C4I system in a systems engineering simulation of the wargame to see how well the C4I system collects the required information. Third, a operational commanders now play through the wargame scenario, making decisions

---

[58] Although not cited by M. Sovereign, W. Kemple, and J. Metzger in "C3IEW Measures Workshop II," *PHALANX* 27, no. 1, (March 1994), 10-14, the author participated in the workshop and provided much of the work that was adopted in Figures 4, 6, 9 and 10. In fact, Figure 10 was entirely created by the author and briefed by the author to the workshop.

based on the information that the C4I system could actually provide. Finally, the commanders' decisions would be put into a combat simulation where their decisions could be implemented by simulated forces and the impact of the decisions on the battle outcome could be determined.

Another approach that has merit is to consider that the basic purpose of C2 is to recognize and respond to the development of situations. Using this idea, in exercises or simulations, testers could script situations to develop at specified times and then measure the ability of the C4I system to support commanders in recognizing the situation and then planning and executing an appropriate response. In this kind of a test, a better C4I system would recognize a situation in significantly less time than an inferior system and would reduce the time necessary for planning and executing an appropriate response.[59] For example, a situation might be scripted where a new threat force is introduced to the battle space that is a clear danger to the friendly force. Testers could measure how long it takes for the C4I system to support the recognition and response to the threat. Of course, one of the challenges to such tests is the involvement of people in the command and control process which can skew results by errors in human judgment. Fortunately, much work has been done in the human-machine systems discipline and many techniques have been developed for designing experiments to control for training and other human judgment effects.

A third approach that is gaining favor would involve the user and tester working together much earlier in the acquisition process to define the missions that the units and forces are expected to achieve when outfitted with the new C4I equipment or system. Then

---

[59] Philippe H. Cothier and Alexander H. Levis, "Timeliness and Measures of Effectiveness in Command and Control," *IEEE Transactions on Systems, Man, and Cybernetics* SMC-16, no. 6, (November/December 1986), 844.

together with the user, the tester would develop a template for evaluating whether or not a mission was successfully performed.[60] For example, a new reconnaissance platform might have, as one of its missions, to conduct an area reconnaissance of a specified size area. The mission success template might specify the percentage of enemy units in the area that must be correctly detected and the time constraint for accomplishing the detections. An advantage of this mission-template approach is that it makes the comparison of competing C4I equipments and systems easier by simplifying the arguments about operational effectiveness. The system with the significantly higher mission success rate across different scenarios is the more effective system. Then acquisition arguments can focus on the easier questions of operational suitability which is generally much easier to determine in testing.

Still, as Charles Hall points out, there are several difficulties with the mission-template approach.[61] First, there is much interaction between mission accomplishment and tactics especially with new systems with new technology. A new C4I system may require the development of new tactics, techniques, and procedures to take full advantage of its capabilities.[62] This fact recognizes the importance of a close working relationship between the tester and the user. One way to provide for this interaction is to leverage information technology advances for virtual prototyping where users can experiment with new systems in a virtual combat simulation environment before the system is even built. This allows the user to develop and practice appropriate tactics. Of course, the new system may provide the

---

60 Hap Miller, interview by author, written notes, United States Military Academy, West Point, New York, 5 May 1994.

61 Charles R. Hall III, interview by author, written notes, MITRE Corporation, Reston, Virginia, 5 April 1994.

62 Charles R. Hall III, "An Approach to the Measurement of the Marginal Contribution of C4I Enhancements to Force Effectiveness," in press, Navy Systems and Technology Division, MITRE Corporation, 5 May 1994.

capability, once in the users hands, to accomplish new missions that were not envisioned in the design or to accomplish old missions in entirely new ways. This rapid prototyping could also improve the requirments generation process since users could discover early-on the practical advantages of new capabilities. Again, the value of prototyping and interaction between the tester and user is evident.

Sage recommends a system quality assurance attribute tree approach for developing metrics.[63] In this approach, quality assurance attributes for the structure, function, and purpose of a system are identified. These high-level attributes are then decomposed into lower level attributes until quantifiable attribute measures can be identified. Once measures for C4I systems are known and tests have been conducted, *evaluations* of the cost-effectiveness of the new system compared with other alternatives must be considered.

Value-Price Trade-Offs

Often difficult trade-off decisions must be made between desired capabilities and costs. For example, there may be existing or planned systems of other services that can meet most of the required capabilities of the new system. Is the cost of a new system really worth the improvement in capability over current or other planned systems? Historically, these evaluations have focused on effectiveness and cost considerations. Today, there seems to be growing concern that more attention should be paid to value and price issues[64] especially for C4I systems. A value perspective emphasizes the *usefulness* of a system. Price emphasizes *choice*. When a choice to buy something is made, something else that could have been bought is sacrificed. But the sacrifice is tolerable because what has been chosen is ***relatively*** more

---

63 Andrew P. Sage. Systems Engineering, (New York: John Wiley, 1992), 159-62.

64 Department of Defense, *Report of the Defense Science Board Task Force on Defense Acquisition Reform*, Office of the Undersecretary of Defense for Acquisition, Washington, D.C., (July 1993), C-2.

valuable to the user. Therefore, a value-price viewpoint considers not only what is being bought but also what is not being bought and is more sensitive to the the subjective evaluation of the user. The traditional cost-effectiveness approach is more objective. Part of the problem is that,

> Government profit 'guidelines' do not encourage contractors to reduce costs since profit is a percentage of cost. On large contracts - especially follow-on contracts - there is little reason to drive down costs since the government will likely reduce the profit accordingly.[65]

Another aspect of the problem is that "unique government processes and specifications often result in the development of unique components and systems rather than commercial standards. This practice often precludes the use of commercial items that are produced in greater quantity and at a lower price."[66]

It seems the government is much better at determining the cost of something but has great difficulty at determining its value. Government buying decisions have historically focused on the lowest cost often, it seems, with a disregard of quality. Of course, the government's responsibility to protect the public interest cannot be ignored. Still, sometimes the initial procurement cost of a high quality system may more than pay for itself due to reduced lifecycle operation, maintenance, and retirement costs. Terms like value and quality are hard to define. As Sage points out,

> Quality is a subjective term and a multiattributed one as well. Simply stated: system quality is the degree to which the attributes of the operational system enable it to perform its specified end-item functions so as to achieve client purposes in acquiring the system.[67]

For software products, Sage believes that it is possible to develop quality metrics for these systems by constructing a tree of attributes that includes such dimensions as purposes

---

65 Ibid., C-5.

66 Ibid., C-4.

67 Andrew P. Sage, *Systems Engineering*, (New York: John Wiley, 1992), 132.

served or performance objectives, operational functions performed, features of the system, and reliability, availability, and maintainability.[68] Importantly, Sage cites Garvin's definition of a value perspective of quality:

> From this [value] perspective, a quality product is one that provides sufficient performance at an acceptable price. This approach blends quality as a measure of goodness [inherent excellence, you know it when you see it] with quality as a measure of utility [user feedback]. Quality, then, can be maximized only for certain customers, unless the product has very universal appeal.[69]

Since much of the strategy for improving C4I systems in the future is focusing on leveraging commercial off-the-shelf products and services, then how should the services determine what to buy? Several answers come to mind. First, the services need to put some of Deming's 14 points on quality into practice. Two seem especially relevant to strategies for acquiring C4I systems:

> End the Practice of Choosing Suppliers Based Solely on Price: The lowest-price components often are not the least expensive ones, especially over the long term. If the lowest-price components are not of good quality and if the vendor does not provide appropriate maintenance services, it is likely that these components will create quality problems, and long run costs will be increased. Deming advocates working with a single supplier when its quality and service meet the needs of the organization. Above all, we should buy for quality and not for price alone.
> Continually Improve Processes: Improving productivity should be a never-ending task. The objective should be not to fix problems once and forever but to commit to continued improvement through process improvement.[70]

It may be difficult for the services to develop a close relationship with a quality conscious supplier as Deming advocates. One way the Japanese have implemented this part of Deming's philosophy is by developing a relationship with two or three quality suppliers for each critical component they need. In this way competitive tension is maintained as the three suppliers work hard to win the major share each year. Some criticize this approach since it

---

68 Ibid., 193.
69 Ibid., 195.
70 Ibid., 214.

might not allow smaller firms to compete. However, perhaps the contracts could stipulate that the three main suppliers outsource a certain percentage of their work to smaller firms. In this way, the government would benefit by having a dependable supplier and would not have the overhead of working many small procurement contracts. This would be accomplished in a more efficient way in the free marketplace, with much less red tape, by the three major suppliers working with smaller firms.

In summary, the goals that should drive value-price strategies for C4I systems acquisition and integration are:

1) To identify new technology approaches that enhance functionality and usability of the new system.

2) To identify significant "price-drivers" that represent a high percentage of total costs of the system.

3) To identify methods that reduce costs while simultaneously retaining needed capabilities and on-time delivery of the operational system.

4) To field a quality system, within the constraints set by schedule and price, that is interoperable, compatible as needed with existing legacy systems, and has potential for growth using future technologies.

5) To establish a process for ensuring continuing functionality and usability of the system throughout the system's life.[71]

Establishing a process that has the necessary configuration management controls, with appropriate audits, reviews, standards certification and accreditation all takes time and resources.

Time and Resources

Therefore, a major issue in testing is the time and resources that can be committed to such efforts. The interviews suggest that usually too few resources are available for tests and

---

[71] Adapted from Andrew P. Sage. Systems Engineering. (New York: John Wiley, 1992), 173.

too much time is devoted to evaluations. Because few resources are available, many tests begin with false starts until it becomes clear to higher authorities that the testing will be unsuccessful unless more resources are put toward the effort.

Since identifying technical components and solutions early in a C4I systems acquisition can make it obsolete when it is finally fielded, it seems that many parts of a C4I system would be better pre-tested by undergoing a certification process. A certification process verifies that a particular component has a proven design with very little risk and has performed well in commercial environemnts that are similar to the intended military uses. Such off-the-shelf components need very little testing except to make sure they comply with standard architecture specifications. In this way, C4I equipments could be placed into a catalog once they had been certified. These equipments could then be integrated into C4I systems without the necessity for detailed testing. This would save time. Companies could pay for the certification process and would be motivated to do so by their competitive desire to have their products listed in the catalog. This would save money. Some aspects of the certification process might be as simple as documenting that the products were operating in the commercial sector in similar environments and were subject to the same standards. For example, a software product that is being used commercially in an environment or architecture that meets or exceeds DOD standards is a product that should need little testing.

Since the commercial market is driving the information technologies which form the basis for C4I systems, it stands to reason that the commercial sector must also perform extensive testing. Evidence shows that entire industries are being created to help commercial

hardware and software developers test their wares. Therefore, exploring ways to use commercial testbeds for DOD purposes seems promising.

One of the major problems with resources for testing and evaluation is that the resources that must be dedicated to these efforts are very visible while the benefits are not. Therefore, managers tend to be shortsighted in their allocation of funds to testing and evaluation. Perhaps by adopting the "build a little, test a little" philosophy, managers will be able to see the payoffs from rapid prototyping and will be more supportive of testing and evaluation. Instead of making the tests part of a big obstacle to overcome near every milestone decision, testing and evaluation may be better accomplished incrementally throughout the system development process.

CHAPTER IV

USER PERSPECTIVES

Two issues dominated the concerns of users: compatibility and usability.

Compatibility

It is easy to understand why compatibility is an important concern from a user perspective. When two computers are compatible, "they will produce the identical result if they run identical programs. Another meaning is whether equipment, peripherals and components, can be used interchangeably with each other, from one computer to another."[72] Besides computer compatibility, there are other types of compatibility. For example, electronic equipment or systems are said to be electromagnetically compatible when they can be "used in their intended environment within designed efficiency levels without causing or receiving degradation due to unintentional electromagnetic interference (EMI). EMI is reduced by, amongst other things, copper shielding."[73]

EMI can be particularly troublesome where limited space is available for locating C4I equipments, such as on Navy ships. In the Falkland Islands War, for example, British guided-missile destroyers had to shut down their satellite communications system since it could block out their detection of the radar on attacking Argentine Super Etendard jets armed with the deadly anti-ship Exocet missile.[74] In fact, the first ship that the British lost in the

---

72 Harry Newton, *Newton's Telecom Dictionary*, 1993.

73 Ibid.

74 Sandy Woodward, *One Hundred Days: The Memoirs of the Falklands Battle Group Commander*, (Annapolis: Naval Institute Press, 1992), 7.

Falklands was the H.M.S. Sheffield and as Admiral Woodward explains, "Problem number one was that she had been transmitting on her SCOT satellite communications system at the critical time when the Etendards' radars were used. This blotted them [attacking jets] out in Sheffield."[75] What users want is to be able to use and operate equipment that works seamlessly together, not just "functioning without mutual interference" but complete compatibility. Unfortunately, there are many obstacles to compatibility for C4I systems.

Setup, installation, and initialization difficulties plague C4I systems. Apparently, the main cause of these difficulties is the many different vintages of C4I equipments existing in the military forces at any one time. For example, in Operation Desert Storm, there were a number of different generations of communications systems deployed which had to be linked with different vintages of commercial communications equipments that had to be patched together.[76] Making the problem worse is that real operations always seem to require more C4I equipment than planned. Again in the Persian Gulf War, higher echelons had requirements to establish communications connectivity with coalition forces. Also, within US forces, many more computer and communication terminals and communication links were needed at every echelon than anticipated by acquisition and fielding plans. As a result, lower echelons often had to give up or dedicate organic equipment to meet higher echelon taskings. Also, military users discovered many more uses of C4I equipments through day-to-day operational experience.

Although it is possible and desirable to think of ways to reduce the different vintages of C4I systems and equipments, such as open architectures and "plug and play" technologies,

---

75 Ibid, 13.

76 Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress*, (Washington, D.C.: U.S. Government Printing Office, April 1992), K-46-9.

it is very likely that these problems are an operational fact of life. So C4I systems should be designed and fielded with the expectation that more nodes and more links to and from different vintages and echelons will always be an operational requirement. Therefore, requirements that address backward, lateral, and upward compatibility are mandatory as well as the requirement to expand easily.

What would some of the features of a compatible, expandable C4I system be? First, it should be easy to identify, assemble and connect the hardware components of such a system into a network. Similar to the AppleTalk network approach, the cables, cable ends, sockets, connector boxes, and terminals should be labeled with small pictures or icons so the parts can be plugged together quickly. Components of such a system would have built-in circuitry for connecting computers, printers, and other devices to a network so that users can share information and resources. Expansion slots on system components would provide places where a circuit card can be installed to provide a connection to a different type of network if needed.

Second, the software for such a system would quickly diagnose what hardware components were connected and would self-configure to support operations. The software would help installers and operators customize and tailor the network and its resources appropriately. For example, network file servers, which are computers with powerful processors that can expand access to programs and data significantly without adding any components to other computers on the network, would run software to manage themselves. This software would create restricted files on the server and designate who will have access to

them and protect access to the use of the file server by password security and designating specific sets of users and computers as virtual nets.

Usability

User interfaces and user friendliness are the main concerns of operators of C4I systems. Since computers exist throughout C4I systems, most user interface frustrations focus on the ways people must interact with computers. An often heard complaint is the lack of consistency across systems, operating environments, and applications. For example, one former executive officer of an aircraft carrier complained that even within his ship there were many different interfaces which made each station operationally unique. An analogy to this problem might exist if every car had a substantially different interface between the driver and the car. For example, instead of every car with a steering wheel, brake pedal on the left, gas pedal on the right, with settings for park, reverse, and drive configuration, what if some had a steering bar for your feet with hand levers for braking and acceleration? Certainly, there would be the need for much individualized learning and education depending on the car one had to drive. The fairly consistent user interface design of the automobile greatly reduces training requirements and helps to avoid costly accidents.

Fortunately, user interfaces for computers are moving to a graphical users interface (GUI) standard that was pioneered by Apple with the Macintosh. WINDOWS by Microsoft has made the GUI available to the MS-DOS (Microsoft Disk Operating System) computing world. Most other computer interfaces have moved or are moving to a GUI direct manipulation interface. What makes this emerging standard so appealing is that all applications have the same "look and feel". Many tasks that are common across applications,

such as saving or printing a file, can all be accomplished in the same way. This permits users to learn new applications very rapidly as much of their knowledge is transferable. As an illustration of how far the Macintosh environment takes this idea, here is an excerpt from their manual, "Most important, you use about two dozen simple operations to work with your Macintosh, and these operations are the same regardless of the program you're using or the task you're performing."[77] Still, there are many service and system unique computer interfaces that are very different. For example, many acquisition radars have computer displays with unique symbology. Across services, some radar symbols depict a friend in one system which is the symbol for a foe in a different services radar display.

Many advantages would accrue to the services if they looked across services and systems to identify common functions and tasks. Then designing C4I systems that have user interfaces with the "same look and feel" would reduce training costs and enhance system acceptance and usability. For example, every service has the need to exchange administrative electronic mail (E-mail) messages. How many different E-mail applications with different interfaces are now in use?

The commercial sector has been working hard on making systems easier to use because they realize that most modern systems do not fail for lack of functionality. Instead, most systems are unsuccessful because they are too hard to use. This means that systems today will usually be able to do everything they are supposed to do. The problem is that sometimes, the difficulty of getting the system to do what one wants will be so burdensome, that users will revert to an older system or even a manual system to accomplish their tasks. This is where systems can fall short of user expectations even though the system meets the

---

[77] Apple Computer Inc., *Macintosh Reference*, (Cupertino: Apple, 1989) 2.

user's functional requirements. For example, a version of the Army's Maneuver Control System was supposed to provide the user the ability to create operations overlays electronically. MCS did allow users to create all the necessary symbols for making an overlay except it took many convoluted series of keystrokes and inputs to create even one symbol. What could be drawn by hand in a few seconds, like an axis of advance arrow, took two hundred times longer, twenty minutes, using the MCS. As a result, users much preferred the manual method. Therefore requirements need to include usability as well as functionality.

One way the commercial sector is improving usability is by establishing usability centers. Miller explains,

> Typically these studies [usability tests] are done in special rooms with one-way mirrors, either at the developers' site or at a company that specializes in usability tests. Test subjects come in and run through a series of tasks, while the developers of the software watch them through the mirror and monitor their reactions...software developers watch to see whether the test participants can easily understand the user interface and the on-screen instructions. After all, seeing exactly where potential customers have trouble understanding what to do is much more effective than simply hearing how difficult it is from a technical-support line, a written review, or an on-line forum.[78]

User friendliness is the other part of usability that concerns operators and commanders who use C4I systems. Most complaints say that C4I systems are too rigid and are not flexible enough to accommodate different command styles and the many changes which occur in battle situations. The cause of most of these difficulties is the lack of appreciation that designers and developers have for the operational environment of the military user. What makes this job of understanding more difficult is the differences among the services' command and staff cultures as well as the obvious differences in their warfare environments.

---

[78] Michael J. Miller, "The Myth of Usability," *PC Magazine*, 12 April 1994, 79-80.

The result of not understanding these differences is that C4I systems are put into operation that support the thinking process at the wrong level of abstraction for combat operations. Again, using the automobile analogy, consider that there are several different perspectives or abstractions of reality about a car that are useful. For example, an automobile mechanic, in diagnosing and repairing problems may think about the electronic ignition system and tracing voltages. A body repair technician would concentrate on the fit and finish. But, the operator of the car would soon have an accident if they had to think about stopping a car by tracing through in their mind the inner workings of the braking system. Instead, drivers think about speed, braking distance and when to step on the brake pedal, a very different level of thinking about the car than the engineer that designed the braking system. Of course, the successful driver interface that supports the thinking at the correct level of abstraction for the driver, developed over many years.

Many of our C4I systems have artifacts designed in their user interfaces that support thinking at the engineer and technician level instead of at the commander and military operator level. For example, one C4I system had a key labeled "db init" which had something to do with initializing a database so that the system could receive information from other elements and make displays of the information on-screen for commanders and staff officers. To really understand what this all meant, a soldier needed, if he was to understand it as "db init", to know about distributed data base constructs. The soldier could have accomplished the same task by a simple key that said "unit". Upon pressing the key, the soldier could have been asked simple questions by the system about his unit that would have accomplished the necessary data base initialization. The point here is that C4I systems need to be designed in

the operational language of the warfighters that position and operate military forces. In other words, systems should support thinking and decision making in terms that are familiar to the user and consistent with the user's perspective on the operational environment.

Consider the metaphor that is being used by most graphical user interfaces today. It is a desktop or notebook metaphor. There are folders and clipboards and many icons that represent routine thinking in an administrative office environment. One has to believe that there is a more powerful metaphor that could be used to support the real-time decision making required in battle situations. The question for C4I systems is what metaphor is appropriate for the different warfare environments in which commanders and warfighters must operate? According to an expert interface designer, "The best metaphors are the simplest ones that tie concretely to our world."[79]

Earlier, command and control was described as a process of recognizing and understanding situations, developing and disseminating plans, and executing and monitoring combat operations. Also, it was said that command and control is all about decision making. Hence, a good question is what are the decisions that take place in the command and control process and what difficulties do commanders and warfighters face in making these decisions? Such an understanding is very important since C4I systems must be designed to help the commander cope with these difficulties.

Frank Snyder describes the decisions that take place in the command and control process in terms of three types:

> operational, organizational, and informational. We customarily think of commanders as focusing primarily on operational decisions about the employment of their forces, but such decisions are made only in light of prior organizational and information

---

[79] John Kador quoting Dr. Susan Weinschenk in "One on One," *Midrange Systems*, 11 February 1994, 46.

> decisions. Prior organizational decisions have established a chain of command for the execution of operational decisions, as well as establishing a structure for the flow of reports, and for the intermediate processing of information. Information decisions are made by commanders to establish what they believe the situation to be, and how that situation relates to the mission they are trying to accomplish. Although information decisions are not always articulated, a commander's operational decisions (about what actions subordinate commanders are to take) are always preceded by information decisions about what is actually happening[80]

Informational decisions are the commander's assessments of the developing situation and what it means in terms of mission performance. Hence, the intelligence system plays a major role in supporting these informational decisions. The question for C4I system designers is how well do their designs help the commander make situation assessments? Is the intelligence system an integral contributor to that decision making process or an intermittent participant? Since, as Snyder points out, these informational decisions are sometimes not articulated, should C4I systems help make the commander's situation assessment decisions more explicit and visible to reduce the possibility for misunderstanding and confusion? These are important questions for designers to consider.

Organizational decisions are how the commander decides to establish the chain of command and organize units and forces to provide information and execute actions. It is interesting to note that although military organizations are organized in very strict hierarchical fashion, commanders have a great deal of freedom in organizing their forces. For example, normal practice is for commanders to meet at least once a day with their staff and sometimes subordinate commanders are asked to attend. In this meeting, the current situation, future plans, and on-going operations are usually discussed. Commanders have complete freedom to decide how to structure these meetings. Since these meetings can have a significant effect on

---

[80] Frank M. Snyder, *Command and Control: The Literature and Commentaries*, (Washington, D.C.: National Defense University, 1992), 13.

what information is exchanged and therefore what decisions, if any, get made. The main point is that commanders have considerable flexibility in organizing their commands and C4I systems need to be flexible enough to support the tailoring of the organization by the commander. Also, the C4I system should help the commander understand the advantages and disadvantages of different organizational structures. Simple concepts, such as the delays in reporting information that may be inserted into an organization by multiple levels of hierarchy, must be understood by the commander.

Operational decisions concern deciding on courses of action and determining when to change orders or plans. Some work on C4I systems focuses on whether or not the operation is proceeding as planned. Some evaluations even focus on how long a plan can last. The assumption is that a better plan must last longer. However, some argue that the real question to ask is whether or not the objectives of the operation are being achieved.[81] Others point out that planning is entirely situation dependent. In some cases, staying with a plan a long time may be the absolutely wrong thing to do. In other cases, because of the high cost in time and effort required to change an operation in progress, it may be best to stay with even a poor plan.

In summary, C4I systems need to support three main decision making functions: assessing situations, developing and disseminating plans, and executing and monitoring operations. While supporting these functions, C4I systems must be flexible enough to accommodate the various organizational structures that individual commanders may prescribe.

---

[81] Frank M. Snyder, interview by author, written notes, Naval War College, Newport, Rhode Island, 5 May 1994.

Functionality is not, however, enough. C4I systems must be easy to use. Only a thorough understanding of the commanders' and warriors' operational environment will ensure usability.

CHAPTER V

C4I SUBSYSTEMS AND LESSONS FROM THE PERSIAN GULF CONFLICT

This chapter presents several interesting observations related to the various subsystems of C4I and highlights command and control lessons learned from the Persian Gulf Conflict.

Communications Systems

Advances in information technology are making communication much more of a personal asset than an organizational asset. Personal communications assistant technology[82] will, in the future, be available to almost every person similar to the way a telephone is available now to every household. This spread of personalized communication technology worldwide will create a C4I leveling effect among military forces. Potential adversaries will be able to buy or lease communication capabilities that approach or equal those of US forces.

Commercial space-based communication networks such as Motorola's Iridium project[83] and the Gates/McCaw Teledesic[84] project will provide mobile communications

---

82 Personal assistant communications technology is the integration of a mobile telephone with a small computer device.

83 Iridium is a 3.3 billion dollar satellite telephone system being put together by Motorola Corporation. The system will consist of 66 satellites in geosynchronous orbit that will provide the capability of providing mobile voice conversations and electronic mail deliveries for people with laptop computers and cellular-like telephones or the combination of the two devices, a personal communications assistant.

84 Teledesic is a 9 billion dollar satellite communications system being put together by Bill Gates of Microsoft fame and Craig McCaw of McCaw Cellular Communications. Together the two represent the largest software company and the largest cellular telephone company in the world. The purpose of Teledesic is to deliver high-capacity bandwidth communications connectivity, similar to land-based fiber optic networks, to even remote areas of the world. Users of the Teledesic system could transport high-resolution images or two-way video conferences to and from anywhere on the globe. To achieve this quantum leap in capability, Teledesic will deploy 840 small satellites in clusters of low earth orbit. Since Teledesic will communicate using ultra-high radio frequencies, large numbers of satellites are needed to overcome atmospheric interferences and to provide global coverage.

support to even remote areas of the globe. On the ground fiber optic cables will dominate the infrastructure. Fiber optic cables will be integrated into building structures, highways, bridges, tunnels, ships, and even vehicles. The combination of these two technologies, commercial satellite and fiber optic communication networks, will cause the co-mingling of communications on a scale difficult to imagine. It will be very hard to identify message traffic to particular users such as special interest groups or even nations. Trying to deny communications to particular groups of users or nations will be increasingly difficult and problematic. Severing or denying communication links will be difficult and politically troublesome as many interested friendly parties would receive collateral damage due to such interference. Intercepting communications will be difficult since the spread of advanced computing technology around the globe will provide enormous encryption capabilities to potential adversaries. The advance and globalization of communication technologies will greatly complicate intelligence collection efforts. Monitoring these vast communication networks will require much more capable control systems.

Control Systems

Control means that feedback about operations is available so actions can be taken to make sure everything is going according to plan or at least that some progress is being made toward designated objectives. However, control can also be applied to C4I systems themselves. Because C4I systems are becoming increasingly complex and more and more people and computers are being tied together by computer-communication networks, systems to control C4I systems are needed. Consider this example and imagine what consequences might occur if something similar happened to a battlefield C4I system:

> In June 1990, millions of US telephones went dead because of three lines of faulty computer software code (out of more than 2 million). Those few mistakes set off a chain reaction involving three Bell companies using the software for call routing. As a result, an electronic traffic jam paralyzed the phones of 10 million people in Los Angeles, Pittsburgh, and Washington.[85]

Unfortunately something similar did happen, luckily the scale of the incident was much smaller but still tragic. During the Persian Gulf War, a software error in the command and control complex of the Patriot missile system was responsible for "throwing off the radar's timing by one-third of a second, causing the Patriot to miss an incoming Iraqi Scud missile that killed 28 soldiers and wounded 97 in Saudi Arabian barracks."[86] Such incidents should be adequate warning that control systems for C4I systems are needed. Another example comes from Canada. Apparently the Canadian National Railways systems could be

> crippled in the Year 2000 if steps aren't taken to resolve a problem relating to rollover date changes on as many as 66 systems. The systems control everything from locomotive repairs and Intermodal equipment to customer waybills. The problem involves two-digit date fields which are used in thousands of legacy systems on mainframe and midrange computers. After January 1, 2000, without a four-digit date field to reflect the new century, the systems could crash.[87]

Intelligence Systems

The most frequently cited problem with intelligence in C4I systems is the separation that exists between operations and intelligence. Commanders and their operations staff seem frustrated by the "green door effect." This means that commanders and their operations officers tend to think that intelligence officers withhold too much information in the interest of protecting sources and in support of compartmentalization policies. For example, the model for the intelligence cycle normally depicts a commander asking a question to start the cycle. The cycle progresses from asking a question, which generates an intelligence requirement

---

85 Carol Minton, "War Stories on the Software Testing Front," *MIDRANGE Systems*, 11 February 1994, 28.

86 Ibid.

87 Ibid.

which in turn starts an intelligence system collection and analysis effort, to ultimately and finally, providing an answer. Commanders see the intelligence process as being too dependent on this reactive cycle. Instead of an intelligence effort that waits for a question to be asked, commanders would much prefer one that anticipates the commander's information needs. Further, intelligence officers are sometimes accused of not staying abreast of current operations and future plans. Therefore, they do not produce timely, meaningful information. Currently, the only way this problem is made better is by a proactive intelligence officers dividing their time between the two functions: operations and intelligence. C4I systems need to be designed to overcome the barrier between intelligence and operations. Protection of sources and compartmentalization of information, since they are largely bookkeeping and recordkeeping tasks that are good candidates for automation, should be transparent to operations officers .

A problem recognized in Desert Storm is the dissemination of information to lower level commanders. There were two aspects to this problem. Senior level commanders hold most of the intelligence collection assets that can generate detailed information at their level. However, since their information needs are generally better served by information that has been aggregated to suit their needs, many important details are summarized out of the intelligence before it is disseminated to lower echelons. As a result, lower level commanders find the summarized information of little use. Further, disseminating information through levels of command generates delays. Although the higher echelons generally have a longer planning horizon and have more time to compensate for intelligence developments than lower echelons, it is the higher echelons that get information soonest.

The other problem with disseminating information generated by intelligence assets is that lower echelons often do not have the equipment to electronically receive information that is being broadcast. Desert Storm revealed a real need to proliferate more receivers to lower echelons so they could receive broadcast intelligence in a timely manner.

Command and Operations Centers

Contrary to the disciplined teamwork procedures that commanders and warriors usually follow when prosecuting engagements, many important control functions are carried out in group settings. These command and operations centers are subject to all of the problems and advantages associated with groups. For example, strong personalities can dominate a group and cause thinking to be directed in a particular way even though that strong personality may not have a knowledge base to support that thinking. "Group think" can occur where normally very rational people can adopt risky and irrational attitudes due to the protection offered by a degree of anonymity and surreal discussions that occur in groups. C4I systems need to be designed that will guard against the disadvantages of group behavior and that will enhance the benefits of group work. For example, returning to the Blackhawk shootdown described in the first chapter, some evidence suggests that the AWACS crew lost track of the two helicopters in a hand-off among crew members. According to the report,

> The Blackhawks initially were in contact with the Air Force AWACS plane monitoring the area, but were flying so low that the AWACS radar lost contact with them. When they reappeared on the radar, another air controller aboard the AWACS didn't recognize them and summoned the F-15s to investigate. The fighters identified them as Iraqi Hinds. The controller asked them to make additional passes to confirm the identification, which they did. After several more passes, the F-15s were told to fire on the helicopters.[88]

---

[88] Thomas E. Ricke, "US Fighters Accidentally Shoot Down Two American Helicopters Over Iraq," *Wall Street Journal*, 15 April 1994, 10.

A well-designed C4I system might have prevented this mistake in several ways. The AWACS system could have alerted the controller to the missing friendly tracks that had not reappeared. The F-15 could have taken video images of the helicopters and communicated the images back to the AWACS for identification by a computer with a high-speed pattern matching algorithm which would compare the images taken by the F-15 with all known helicopters in the world. Even though predicting future capabilities may be interesting, a look to the past can also be helpful.

In summary, command and operations centers are often put together in an ad hoc fashion and do a poor job of understanding how their personnel should work together as a team. Most operations centers have too many people involved in their processes. This has two detrimental effects. More people bring in more information and insert more delays into the information processing of the center. Therefore, it takes longer to find important information and longer to process it. Also, everytime a human transmits or transcribes information, there is the opportunity for error.

C4I Lessons of the Persian Gulf Conflict

Many accounts of the Persian Gulf Conflict describe how coalition forces, led by the US., orchestrated the decapitation of the Iraqi command and control system while achieving an unprecedented advantage in collecting and exploiting information.[89] What were some of the major successes related to command and control that made this possible?

Major Successes. First, several new systems provided coalition commanders a significant advantage in recognizing and understanding the situation and in finding targets.

---

[89] James S. Cassity Jr., "Command, Control Advances Permeate Combat Successes," *Signal Magazine*, (May 1991); James W. Canan, "How to Command and Control a War," *Air Force Magazine*, (April 1991); Timothy J. Gibson, "Command, Control System Abets Victory in Gulf War," *Signal Magazine*, (March 1992).

The Joint Surveillance and Target Attack Radar System (JSTARS)[90] helped give commanders a large-scale overview of the area of operations. JSTARS detected and monitored major enemy ground movements and helped to locate and track high-value fixed and moving ground targets such as logistic sites and Scud missile launchers. Here is an impressive example of how JSTARS improved situation and target development.

> On 29 January, JSTARS detected a convoy moving south from the suburbs of Kuwait City. JSTARS tracked the convoy and passed the target to the Airborne Battlefield Command and Control Center, which called in Coalition aircraft. These aircraft reportedly destroyed 8 of 61 vehicles in the convoy. Later that day, during the battle for Al-Khafji, JSTARS confirmed no Iraqi reinforcements were being sent, permitting a rapid and accurate assessment of the tactical situation which helped in the plan for the counterattack.[91]

Another new system that made a major contribution in helping commanders understand the situation was the Global Positioning System (GPS). GPS is a system of satellites coupled with ground control antennas that provides navigation and positioning data to hand-held receivers. These small hand-held devices had an enormous impact on improving command and control in the difficult-to-navigate, featureless desert. Using GPS, virtually every friendly unit knew and reported their location with pinpoint accuracy. Despite the lack of man-made or natural features to aid navigation, commanders, in this conflict, thanks to GPS, had a much better understanding of the friendly situation. Moreover, the command and control advantages of GPS were widespread across the force. The more than 5000 GPS receivers deployed to the Gulf,

---

[90] JSTARS is an airborne radar and communications system installed in a military version of the Boeing 707 aircraft. A flight crew of four plus 17 to 25 mission specialists process, analyze and disseminate wide-area surveillance and targeting information to ground and air commanders. In addition, ground station modules (GSM) located with various command and control centers have the same radar picture available to on-board operators via a surveillance control data link (SCDL).

[91] U.S. Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress*, (Washington, D.C.: U.S. Government Printing Office, April 1992), T-86.

> were used throughout the theater to assist forces at sea, on land, and in the air. For example, GPS fixed navigational positions during mine clearing operations and provided launch coordinates for ships firing TLAM [Tomahawk Land Attack Missile]. Among other uses, GPS guided maneuver units, helped minimize fratricide, registered artillery and precisely located land mines.[92]

These new systems were synergistic. For example, JSTARS controllers communicating with pilots whose aircraft were equipped with GPS, were able to accurately guide pilots to targets and recommend the most advantageous attack positions. More evidence of the synergistic effect of GPS is that the United States was unable to satisfy the demand by military users for the device despite off-the-shelf purchase of thousands of commercial receivers. Obviously, many more military applications for the device were invented by users in the conflict than were envisaged by the developers of GPS. In fact, one recommendation from the Persian Gulf Conflict was that GPS should be incorporated into all weapon systems and platforms.[93]

The importance of space-based systems to success in the Persian Gulf Conflict cannot be over-emphasized. Two systems, LANDSAT (Land Satellite) and DMS (Defense Meteorological Satellite), were particularly important for planning. LANDSAT provided detailed images of the earth's surface that were used to create updated maps to show existing manmade features as well as natural terrain and subsurface water features. The multi-spectral imagery data provided by LANDSAT was "...used to plan military operations, and to train and prepare for strike operations and provided unique information on Iraq's order of battle."[94] Shortcomings of LANDSAT are its resolution and responsiveness.

---

92 Ibid., T-227.
93 Ibid., T-229.
94 Ibid., T-232.

DMS provided weather satellite data to coalition forces which was used extensively in planning and executing combat operations. The weather information provided by DMS

> ...became especially crucial in the desert where heavy coastal fogs and sandstorms reduced visibility to zero and rains turned desert sands into bogs. Information on rapidly changing weather patterns was crucial to tactical planners. For example, on 24 January, one DMS readout showed Baghdad in central Iraq covered by clouds and Basra near the Gulf coast clear. Approximately an hour and a half later, a second DMS image showed Baghdad clear and Basra overcast.[95]

A shortcoming with the DMS system was that many tactical units did not have access to DMS data since they did not have any receiver terminals and since higher echelons sometimes took too long in disseminating DMS data to subordinate units.

Communications, the "grease of operations," were very successful. Military satellite communication systems were the backbone of C2 in the Gulf.[96] Using satellites to relay and connect communication nodes overcame the distance limitations of land-based stations which suffer from interference due to terrain and weather. Space-based systems made communications connectivity possible for commanders at all levels, strategic, operational and tactical. The Defense Satellite Communications System (DSCS) augmented by commercial resources "played a major role in providing command, control and intelligence information during Operations Desert Shield and Desert Storm."[97]

Major Shortcomings. Despite the many achievements discussed above, there were several major shortcomings with command and control in the Gulf. First, battle damage assessment (BDA) was unsatisfactory. The Commander of Desert Shield and Desert Storm, General Norman Schwarzkopf complained in his memoirs about the lack of adequate BDA.[98]

---

95 Ibid., T-220.

96 Ibid., K-31.

97 Ibid., T-224.

98 Norman H. Schwarzkopf with Peter Petre, *It Doesn't Take a Hero*, (New York: Bantam, 1992), 430-2.

It was hard for commanders to know how effective a combat operation had been without detailed information on what targets were damaged and the extent of the damage. Also, even when BDA data were available, it was difficult to determine which weapons had accomplished the damage. Some newer systems like the F-117 Stealth aircraft had on-board mission recording devices that made the collection of BDA data much easier.[99]

The second major shortcoming concerned problems encountered in disseminating intelligence collected by national and theater assets to tactical commanders. This was particularly frustrating for tactical commanders since many of their organic intelligence collection assets were tasked away from them by the theater commander. For example, tactical commanders had an "insatiable appetite imagery and imagery-derived products that could not be met."[100] This demand for imagery was made worse by the inability for the component commands (Army, Navy, Marine, and Air Force) to disseminate the imagery that was collected by national and theater imagery reconnaissance platforms. Apparently the secondary imagery dissemination systems of the component commands were incompatible with their subordinate unit's systems. In fact, even couriers were used.[101]

Another shortcoming identified in the Gulf was the ability to find and locate high-value mobile targets such as Scud missile launchers. As evidence of this difficulty, fully one-third of all air sorties flown in the Persian Gulf were dedicated to finding and destroying Scuds. To understand the disruption that this limitation had on intelligence collection efforts, consider this:

> The mobile Scud threat was a case in point. The CINCCENT [General Schwarzkopf's] requirement to suppress Iraq's ability to launch Scuds at Israel -- a

---

99 Department of Defense, *Final Report*, T-2.
100 Department of Defense, *Final Report*, C-8.
101 Ibid., C-9.

> threat to the cohesiveness of the Coalition -- required use of the JSTARS in a Scud-hunting role (particularly in western Iraq, from where the missiles were launched at Israel) and use of the OV-1D [Army reconnaissance and observation aircraft] to fill resulting gaps in coverage. This need superseded the corps' requirements for use of the OV-1D.[102]

Hence, tactical commanders were deprived of intelligence collection assets due to the strain that hunting for high-value, mobile targets placed on the theater commander.

More evidence of the tactical commander's need for imagery and the need to disseminate intelligence is the experience of VII Corps with the Pioneer UAV (Unmanned Aerial Vehicle). The Pioneer flies a televison-like camera over the battlefield and sends the video-images to a ground station television monitor. In one of the forty-three UAV missions flown by VII Corps

> a Pioneer located three Iraqi artillery battalions, three free-rocket-over-ground launch sites, and an anti-tank battalion. Since the system still was in the test and evaluation stage of development, it had inadequate communications and down-link capabilities to be completely effective and widely available.[103]

Navy and Marine elements also operated the Pioneer UAV and found that it proved very useful in providing real-time imagery intelligence and targeting data.[104]

Another problem for tactical commanders was that much of the information they received was not detailed enough for use at their level. For example, "tactical units were sent finished estimates and summaries produced for senior commanders rather than the detailed, tailored intelligence needed to plan tactical operations."[105] This forced these commanders to resort to trying to put together different pieces of information into a complete intelligence picture of the situation confronting them.

---

102 Ibid., C-7.
103 Ibid., C-12.
104 Ibid., C-12.
105 Ibid., C-13.

In summary, air and spaced-based systems provided commanders a much enhanced command and control capability which helped them with situation assessment, planning, and executing combat operations. Commanders at the national and theater level benefited the most from these assets since most of the intelligence processing effort was directed at their needs. Tactical commanders found much of the processed intelligence unsuitable since the information lacked sufficient detail. At all levels, commanders wanted more imagery information than could be provided or disseminated particularly at corps level and below.

Although situation assessment was greatly improved over previous conflicts, battle damage assessment continued to be problematic. Subjective analysis and military judgment was the only way to assemble all the various pieces of relevant BDA information (such as satellite imagery, mission reports, deserter reports, and gun camera film) into a comprehensive assessment.[106] Locating high-value, mobile targets such as Scud launchers proved to be very difficult and consumed a large amount of resources. Fratricide, caused by the ability to acquire and kill targets at extended ranges beyond visual identification, continued to be an unresolved problem of modern warfare. Overcoming these limitations and reinforcing the successes of command and control in the Gulf is a major challenge for requirements writers, system designers, system operators, and future commanders.

---

106 Ibid., C-15.

CHAPTER VI

INFORMATION TECHNOLOGY TRENDS

No investigation of the challenges facing the US military in fielding and using C4I systems would be complete without a discussion of information technology trends. These trends have caused many contemporary theorists and practitioners of war to speculate that we are witnessing a transformation in the art of war. Further, one of the main causes of the disconnects was identified to be the fast pace of information technology development. This chapter looks at trends in four categories and explores what they mean for C4I futures.

Information is knowledge created from data. Technology is the organization and application of scientific knowledge to enhance human activity. Therefore, information technology is the application of scientific knowledge to help people work with data, information, and knowledge. There are more precise technical definitions. For example, information technology is the acquisition, storage, processing, transmission, and representation of vocal, pictorial, textual, and numeric information by microelectronics, computers, and telecommunication technologies.

Before examining the trends in information technology, what really is a trend in technology? A technology trend is the general direction that the enhancement of some human activity by science takes over time. To be a significant trend, there must be some order of magnitude of enhancement. For example, some activity must be improved, perhaps made faster or easier, by tenfold. Sometimes a significant trend in technology is capable of

transforming some human activity. That means that the activity can now be done in an entirely new and different way. What are the trends in information technology?

Computer Trends

Computer technology continues to undergo a metamorphosis from a giant centralized organizational asset to an ever smaller, yet more capable, personal model. With respect to hardware, the price has decreased while capability in terms of memory, storage, and speed have skyrocketed. Miniaturization of the microprocessor has shrunk the size of computer hardware. Mainframe computers that have their own computer rooms are endangered species. They are being replaced by smaller but more powerful computers, called workstations, whose central processing units can fit into a pizza box. This hardware trend of increased capabilities in ever smaller packages has one very important implication: the personalization of the computer.

Computer software trends complement computer hardware trends. The tremendous increase in usability is probably the most notable trend in software applications which is likely to continue. Many features in software such as a help function, provide support for novice users.

A very important dimension of computing involves how people interact with computers. Historically, people gave input to the computer by typing text commands using a keyboard and received feedback from the computer by viewing text and numbers on a Cathode Ray Tube (CRT) visual display or monochrome monitor. Gradually, pictures and color were added to enhance this interaction. Interface experts sought to make human-computer interaction easier, more "user friendly" by adding features to the screen

display such as icons, menus, and windows. Multi-sensory interactions, audio, video, and animation, were added to what had been a plain text and numeric display screen. The result of all of this work has been a tremendous increase in the usability of computers.

Microelectronics Trends

Microelectronics trends continue to promise chips, microprocessors, that are faster and denser by orders of magnitude.[107] This means that computers can process and store more information faster and better than ever before. This also means that chips continue to get smaller even as they get more capable. There seems to be several promising lines of development for expecting continued progress in microchip technology. For example, some researchers are combining optics with electronics to achieve speed-of-light processing capabilities.

Telecommunications Trends

Digitization is probably the biggest trend in telecommunications. Converting information to a series of digits, zeros and ones, puts it in a form that can be quickly encrypted with streams of digits, transmitted by bursts of electromagnetic energy, and then received and rapidly processed by computers. Text, sound, graphics and video can all be manipulated in this way.

Another important trend in telecommunications is the move from telephone-based, voice wire technology to computer-based, multi-sensory, wireless technology.[108] In the past, communications over long distances relied on wires and was accomplished by speaking and listening with a telephone. In the future, communications will be free from the restrictions of wire and will involve seeing and listening with portable computer devices.

---

107 Don Lindsay, "The Limits of Chip Technology," *Microprocessor Report*, 25 January 1993, 21.

108 Ron Levine, "Look, Ma, No Wires!" *DEC Professional*, May 1993, 64.

Combinations of Information Technologies

The way information technologies have combined to spawn new technologies is, by itself, a trend. For example, advances in human-computer interaction technologies combined with advances in microprocessor technology have given rise to interactive multi-media technologies. Multi-media is the computerized integration of text, sound, graphics, and video.[109] This means that, for example, an encyclopedia, can come alive with more than just words to describe people, places and things. Now, the sights and sounds that can engage much more of a person's total perceptive senses is possible. Adding human interaction to multi-media permits people to learn by discovery and exploration in a more personalized, non-linear fashion.

Taking interactive multi-media to the next logical step, advances in animation and simulation technology provided the opportunity to create virtual environments. People can now be immersed in a total virtual reality by surrounding their senses with the products of information technology such as head-mounted displays and datagloves. Experts working in the Media Laboratory at the Massachusetts Institute of Technology recognized that "something qualitatively different happens to you when your senses are surrounded compared to when you are simply gazing at (and listening to) a screen."[110] Human beings have a tremendous perceptive ability when all of their senses are involved and enhanced by information technology. Many possibilities for applying these new technologies exist. For example, interactive virtual reality may provide the opportunity for surrogate reconnaissance.

---

109 Steven V. Zepezauer, "Racing into the Interactive Age," *Graduating Engineer*, January 1994, 24.

110 Brenda Laurel, "Anatomy of a Fad; Post-Virtual Reality: After the Hype," *Digital Media*, 29 March 1993, 5.

Networks that evolve into ever larger networks is a trend that is common to all information technologies. Computers and their users are forming into ever larger networks and collaborating on a bigger scale than ever before. Communication companies are joining together to merge satellites with wireless networks with cable networks to cover most of the planet. Dr. Gell-Mann from the California Institute of Technology explains the network phenomena by his theory of complex adaptive systems. These systems have a natural tendency "to form themselves into larger aggregate systems involving new levels of organization and cooperation."[111]

How can information technology trends and lessons learned in the Persian Gulf Conflict help improve military command and control systems? There are seven significant lessons related to command and control that need to be learned. First, C2 increasingly relies on air and space-based systems for acquiring and transmitting information. Several of the important air-based systems were still undergoing testing and development such as JSTARS and UAV. Almost every space-based system suffered from program or capacity limitations. Apparently, the true wartime requirements for these systems had not been identified. Simply stated, there were not enough satellites to cover war requirements and there was not a capability to surge to meet these requirements by accelerating launches. Both satellite inventories and launching system technology are to blame for the lack of a surge capability.

The second lesson is an old lesson learned again. It is the power of broadcasting plus the synergy of proliferating receivers that is as old as radio. Broadcasting is the simple yet powerful idea of "one to many". The success of GPS in the Gulf exemplifies this lesson. One

---

[111] Aspen Institute Forum, "Special Report: The Information Evolution; How New Information Technologies are Spurring Complex Patterns of Change," *Aspen Institute Forum*, 22 March 1993, 6.

satellite system provided navigation and position data to many hand-held receivers. Many other satellite systems in the Gulf, such as LANDSAT and DMS, cited the lack of receivers for the reason that the information collected, although requested by many, could not be used more widely. Apparently, either system architectures with limited foresight or lack of funding prevented the distribution of receivers as widely as needed.

The third lesson highlights the value of imagery and is a reminder that "a picture is still worth a thousand words." Commanders at all levels, despite having access to more imagery than ever before, still wanted more. Communications professionals often cite the substantial increases in communications cost, more bandwidth, associated with imagery. However, advances in communications technology, particularly in fiber optics and satellites, is beginning to reduce communication cost as an issue for providing imagery. The success of Unmanned Aerial Vehicles in providing valuable imagery to commanders is evidence it can be done. Imagery in the Gulf also raised the issue of dissemination.

Dissemination is the fourth lesson. Crucial details are lost when information is processed from higher levels and disseminated to subordinate units. This may be due to the faulty assumption that the solution to a "big" problem contains the solutions to all "lesser" problems. Some way must be found to preserve the necessary detail for tactical level commanders. If not, perhaps providing a means of helping commanders assemble disparate pieces of information should be a capability provided to more echelons. Much of this dilemma can be solved by analyzing the decisions that commanders are expected to make based on their position in the organization and their role in battle. Then, the information necessary to support those decisions can be identified. Of course, not all information requirements can be

identified in advance so their must be a good deal of flexibility built into the system, a way for commanders to pull critical information from a larger repository of information on demand.

Assembling different pieces of information is the fifth important lesson. Commanders at all levels continue to have a need for piecing together information into a coherent picture. Trends in information technology such as multi-media and digitization provide promise that this puzzle assembly capability can be provided at all echelons.

The sixth and seventh lessons are not new but require continued effort. Locating high-value, mobile targets like a Scud missile launcher validates that it is still difficult to "find a needle in a haystack." Information technology presents an interesting dichotomy to this problem, it offers both a solution and more of a problem at the same time. When information technology creates massively parallel computing architecture that can either be reached by high-speed communications or mounted on platforms in theater, then this problem will be more amenable to solution. However, because information technologies makes more and more information available to decision makers, it advances in information technologies alos seem to be creating ever-larger haystacks to sort through.

And finally, fratricide requires combat identification technology to match the extended acquisition and killing ranges of modern weapons. To reduce fratricide, information technology may be able to provide high-speed, microprocessors that can be mounted on all sensor and weapons platforms to quickly fuse and process information from various sources to provide identification before engagement.

How might trends in information technology change the way military command and control is accomplished? Computers are going to continue to be more usable and

personalized. Networks of computers will continue to grow which will help users draw on more resources. Digital, wireless communications links and the trend in microelectronics toward ever more speed and storage in less size can free command and control from bulky, centralized facilities. Mutli-sensory interfaces can make communications less ambiguous and allow work groups to collaborate remotely over extended distances. Interactive multi-media, virtual reality, and simulation technologies will permit planning and rehearsals on fully-featured, geographical virtual environments. The next chapter examines initiatives and acquisition strategies for making these exciting concepts reality.

CHAPTER VII

INITIATIVES AND ACQUISITION STRATEGIES

A number of promising directions have been chartered by DOD, the Joint Staff, and the Armed Services. This chapter looks at each, how they relate to each other and what they mean for mitigating the disconnects and shaping the future of C4I systems.

Department of Defense: Re-Engineering C3I Operations

Defense Management Report Decision (DMRD) 918[112], "Defense Information Infrastructure" of September 15, 1992 has been the major driver for changing the way DOD acquires and supports information systems and C4I systems. DMRD 918 greatly strengthened the role of the Defense Information Systems Agency (DISA) in managing information systems and "called for the consolidation of the central design activities [software applications], the services' purchasing operations, data processing centers, and a number of communications projects."[113]

---

[112] According to a fact sheet prepared by Ron Oxley in the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence on 17 February 1993, "DMRD 918 was initiated to create an end-to-end information transfer capability which is protected, interoperable, and cost-effective. It designates the Defense Information Systems Agency (DISA) as the single central manager of the Defense Information Infrastructure. The objective is to (1) revolutionize information exchange, defense-wide, (2) strengthen our ability to apply computing, communications, and information management capabilities effectively to the accomplishment of the Department's mission, and (3) significantly reduce the information technology burdens on operational and functional staffs. The DMRD required the development of resource and implementation plans to ensure a smooth transition to this new paradigm [centralized management instead of individual service management]. On December 2, 1992, the Deputy Secretary of Defense approved the DMRD resource plan for implementation. This resource plan will be implemented in two stages, which are currently in progress. DMRD 918C was approved by the Acting DOD Comptroller on December 10, 1992 and reflects the decisions made in the resource plan. On January 14, 1993, the ASD(C3I) approved the DII implementation plan, which documents the overall concept of operations of the DII." Initially, tactical command and control systems were exempt from DMRD 918. Increasingly, all C4I systems are coming under the control of DMRD 918.

Another major driver affecting C4I systems was the Corporate Information Management (CIM) initiative started by the Secretary of Defense in November 1990. As Paul Strassman explains, "The primary purpose of CIM is to deliver a modernized, low-cost, flexible and interoperable DOD information infrastructure that will improve Defense capabilities."[114] The main reason for making CIM, now known as the DOD Information Management Initiative, happen was to transition DOD's "present information systems and associated information technology resources to a communications and computing infrastructure based on the principles of open systems architecture and systems transparency."[115] To accomplish this, DISA developed a generic architecture called the Technical Reference Model (TRM). The TRM is not a specific system architecture. Instead it provides a common conceptual framework, defines a common vocabulary, and specifies standards for the development of DOD information systems and associated infrastructure systems.[116] The TRM is not a static architecture. Rather, it will be updated as "new technologies and standards continue to emerge."[117]

Two major initiatives related to CIM are business process re-engineering and the reduction and integration of legacy systems. Business process re-engineering involves using information technology to assist in reviewing and improving how a business operates. Across DOD, the departments and their functional areas are being asked to make a "systematic, reasoned examination of their operations an integral part of the management of their

---

113 Joyce Endoso, "Software Shops Won't Go to DISA; Paige Lets Central Design Activities Revert to the Services," *Government Computer News*, 19 July 1993, 1-2.

114 Paul A. Strassman, Letter to the Editor, *Government Computer News*, 16 August 1993, 30-32.

115 Department of Defense, "Technical Reference Model for Information Management, Defense Information Systems Agency Center for Information Management," Version 1.3., 31 December 1992, 1.

116 Ibid.

117 Department of Defense, "Technical Reference Model for Information Management," Version 2.0 Coordination Draft, 22 June 1993, 1

functional areas."[118] This generally uses a structured analysis technique such as Integrated Definition Methodology (IDEF) which identifies the inputs, constraints, outputs and control mechanisms of their business activities. Then, once a thorough understanding of how the business currently works is achieved, business process improvement techniques are used to eliminate non-value added activities; streamline value added activities, integrate processes, physical assets, organizations, and data to gain savings; align information systems with the DOD Information Management Integration Architecture (the TRM or the reference model which guides all information systems design); and finally, after all business processes have been improved, automate as appropriate.[119] As one source put it, business process improvement "can be summed up in a three-word motto: Simplify, Integrate, Automate."[120]

Applying business process re-engineering to command and control of warfare can be helpful as long as we recognize that command and control warfare is much more dynamic than business practices. For example, most business models and tools, such as IDEF, are static representations and fall short of the dynamic representations needed to understand command and control.

The other initiative, the reduction and integration of legacy systems, is having a major impact on C4I systems. Integration is being accomplished by standardizing the underlying architecture and selecting standard data elements. Reduction of the number of systems for C4I systems has become a major effort called "C2 Migration." This effort includes approximately 21,000 software applications identified by DISA that must be reduced to about

---

118 Emmett Paige Jr., "Re-Engineering DOD's C3I Operations," *Defense 93*, Issue 6, (Washington D.C.: US Government Printing Office, 1993), 18.

119 D. Appleton Company, Inc., *Corporate Information Management Process Improvement Methodology for DOD Functional Managers*, 2 edition, (Fairfax VA: D. Appleton, 1993), 11.

120 Ibid.

600 migration applications. According to one report, DISA's Center for Integration and Interoperability, which is in charge of the migration effort, says the "21,000 legacy applications or stovepipe systems...covers only command-and-control systems and intelligence systems. It does not include acquisition or reserve component systems."[121] Apparently, DOD has a number of applications with identical or similar functionality, "doing the same thing, with data replicated numerous times in various databases."[122] In the fall of 1993, then Deputy Secretary of Defense William Perry asked "the assistant secretaries of Defense in charge of functional areas to accelerate the selection process and provide him a list of standard systems candidates by the end of March [1994]."[123] Emmett Paige Jr. gave four generic evaluation criteria to help the assistant secretaries make their nominations for selecting migration systems: functionality, technical soundness, program fit, and data standardization. Functionality considers whether the system meets the needs of the users. Technical soundness determines if the system meets or can adapt to the DOD integration architecture. Program fit looks at budgetary constraints while data standardization considers whether the system adheres to or can adapt to DOD's data sharing standards. So far, the services have not been able to meet Perry's March 31, 1994 deadline for identifying interim standard systems.[124] Still, the migration effort has lots of momentum. LTG Alonzo Short, Director of DISA, contends that "the consolidation of systems and applications... offers the highest rewards in terms of economics and interoperability."[125]

---

121 Joyce Endoso, "Pentagon Brass Behind Schedule in Nominating Standard Systems," *Government Computer News*, 7 February 1994, 3.

122 Joyce Endoso, "DOD Pushes for Standard Systems," *Government Computer News*, 27 September 1993, 1-2.

123 Ibid.

124 Ibid.

125 Ibid.

These two initiatives, business process improvement and migration of legacy systems have come into conflict. There seems to be a conflict between those who want to "get it right" and those who want to "do it now." Those who want to "get it right" point to the principle of business process improvement which says automation should proceed "only after the underlying business processes have been cleaned-up."[126] In contrast, seeing many opportunities now for eliminating expensive legacy and duplicate systems, some want to immediately collapse these systems, move to "migration systems" and "do it now." Another aspect to the conflict is probably that there is considerable organizational resistance to changing these legacy systems. As a result, entrenched interests that have become comfortable with these needlessly separate systems are probably using the "automate last" dictum to forestall change. Still some resistance may center on legitimate differences among the ways that the individual services must operate.

Besides conflicts over how fast to proceed and what to do first, some controversy over DMRD 918 and CIM developed due to different visions of how far centralization and consolidation under DISA should go and what the real savings would be. Then Deputy Defense Secretary William Perry in May 1993 signed a memorandum that "put on hold the consolidation of the central design activities, along with the services' acquisition shops and some communication projects, pending a review of the 918 effort."[127] Then in July 1993, Emmett Paige Jr. officially returned control of the central design activities to the services.[128] He explained his rationale, "We would not realize the needed reduction in the number of

---

126 D. Appleton Company, Inc., *Corporate Information Process Improvement Methodology for DOD Functional Managers*, (Fairfax, VA: D. Appleton, 1993), 11.

127 Joyce Endoso, "Software Shops Won't Go to DISA; Paige Lets Central Design Activities Revert to the Services," *Government Computer News*, 19 July 1993, 1-2.

128 Ibid.

central design activities simply by transferring them."[129] Paige did allow the consolidation of two central design activities: "the Joint Logistics Systems Center at Wright-Patterson Air Force Base in Dayton, Ohio, will take over design activities supporting wholesale logistics systems, and the Defense Finance and Accounting Service will assume control of all finance and accounting central design activities."[130] Further, Paige has said that further consolidation and centralization may occur if it is "clearly necessary or is the most effective next step."[131] Paige also hopes the "change in the consolidation plan will let DISA focus on taking control of the department's information processing centers and of communications systems planned for inclusion in the Defense Information Systems Network. DISA also will continue work on standards and department-wide security programs."[132]

This partial implementation of DMRD 918 received substantial criticism. Again, Paul Strassman writes,

> DOD capabilities to direct, architect and manage systems integration must be one of the core war fighting competencies of US. forces, especially for information-intensive warfare. That cannot be abdicated to the commercial marketplace [referring to Paige's decision to out-source the DOD integration effort to a civilian contractor]. You kill the master integration competency within DOD and you have killed the warfare-support essence of CIM. Reversing CIM directions and returning to "stovepipe" management of data, applications, and software assets is easy and will be applauded by the existing constituencies.[133]

So where is DOD really going with information management of C4I systems? One leading expert says, when comparing directions across the Bush and Clinton administrations, says,

> I see a different sense of direction. It's focused at the functional level, at getting migration systems. And I see less of a focus in establishing infrastructure-type activities, with the major exception of data administration."[134]

---

129 Emmett Paige Jr., "Re-Engineering DOD's C3I Operations," *Defense 93*, Issue 6, (Washington D.C.: US Government Printing Office, 1993), 17.

130 Joyce Endoso, "Software Shops Won't Go to DISA; Paige Lets Central Design Activities Revert to the Services," *Government Computer News*, 19 July 1993, 1-2.

131 Ibid.

132 Ibid.

133 Paul A. Strassman, Letters to the Editor, *Government Computer News*, 16 August 1993, 30-32.

Joint Staff: C4I For The Warrior

The Joint Chiefs of Staff initiative is called C4I for the Warrior[135] (C4IFTW). This effort focuses on moving from the four service's stovepipe systems to joint interoperable architecture. The main purpose of acquiring this joint interoperable architecture is to provide the Warrior with a fused, real-time representation of the Warrior's battlespace. To create and display the Warrior's battlespace, the Joint Staff envisions leveraging what they call the "Infosphere". The Infosphere is "..a global network of military and commercial systems and networks linking data bases and fusion centers"[136].

In this concept, Warriors will define their own battlespace by "plugging in", "pulling" (on demand) or having "pushed" to them (over the air updating (OTAU) of pre-planned essential elements of information (P2E2I)) timely, relevant information. Real-time battle-space information is a result of fusion, warrior pull on demand, preplanned essential elements of information, and over the air updating.

The Joint Staff does not see this C4I for the Warrior vision happening over night. Instead, they plan three phases to guide the effort. The first phase is called quick-fix and has already been accomplished. The quick-fix stage has three parts: using translators and interpreters to achieve database interoperability; synchronizing C4I requirements and architecture by requirements certification, interoperability testing, and security accreditation;

---

134 Joyce Endoso. "He's Off I-CASE Buy But Not the Program," *Government Computer News*, 7 March 1994, 14.

135 One very good question about this initiative is who are the warriors and how many are there? Although the Joint Staff has not made this very clear, warfighters seems to mean the combatant CINCs. Warrior seems to have a much broader connotation and means not just commanders of large combat forces but also includes those committed at lower echelons that actually engage the enemy in direct combat.

136 Albert J. Edmonds, *C4I for the Warrior: Committed, Focused, and Needed*, June 12, 1993, The Joint Staff J-6.

and establishing joint interoperability policy and doctrine such as "all C4I systems are considered for joint use." The second phase is a ten year effort called the mid-term transition phase. It focuses on migration planning to phase out remaining "stovepipe" systems and other "baseline" systems based on key migration parameters. This midterm phase fits neatly with Paige's current emphasis on C2 migration systems. The third and final phase is called the Objective Phase and represents the full realization of the C4I for the Warrior vision. The Chairman's instruction paints an interesting picture,

> The technology available during this phase will change the art of conducting warfare significantly. The full implementation of the C4IFTW concept produces a common worldwide infosphere for a single DOD C4I infrastructure. Speed, access, security, display, and menu are terminologies that no longer antagonize warriors seeking information. Warfighters have vendor-neutral, single terminal access to all required information sources. The focus of improvements in this phase is exploitation of the benefits available from advanced technology. Examples include distributed information networks, enhanced onboard processing of miniaturized supercomputers, merging of space-based and other sensor outputs rapidly into tactical systems, and rapid fusion and interpretation using expert systems to support rapid decision making at all levels on the battlefield. The creation of a global C4 infrastructure includes extensive use of commercial C4I systems for day-to-day and surge requirements. It also allows rapid deployment of C4I packages to support worldwide crises...Interoperability is achieved by using software applications independent of the hardware and operating system. Total migration to an open systems environment makes system portability and scalability possible on single integrated terminals that can be used in any warfare environment at any level of command. The transition strategy will shift by using technology as a reason for change.[137]

One example of the quick-fix phase of the C4I for the Warrior vision is based on the idea of "translators" that has appeared in many commercial software applications. The Naval Electronic Systems Engineering Activity (NESEA) found that it could meet the majority of translator requirements for the majority of C4I systems by using a set of just 13 data formats.[138] A technical demonstration of this concept was successful in creating a fused

---

[137] R. C. Macke. VADM USN. Director. *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, Joint Chiefs of Staff Instruction 6212.01, 30 July 1993.

situation picture for all four services by integrating four different service C2 systems. The integrated software system, developed by NESEA, that makes this possible is called the Joint Universal Data Interpreter (JUDI). JUDI converts the various service component data formats to a single format and uses a common language to exchange and fuse information among the components. This is a great example of how applying technology trends to C4I problems can payoff. Imagine the expense of replacing all the service's C2 systems when a relatively simple software solution can have the same result.

Another important Joint Staff initiative is the Global Command and Control System (GCCS). The purpose of GCCS is to take advantage of information technology trends and "move from the proprietary, expensive Worldwide Command and Control System (WWMCS) mainframe computer systems to open, modern, 'client-server' systems."[139]

The final and probably the most important Joint Staff initiative is the Chairman of the Joint Chiefs of Staff Instruction on Compatibility, Interoperability, and Integration of Command, Control Communications, Computers and Intelligence Systems dated 30 July 1993. This document spells out the C4I for the Warrior Objective Vision. The vision has ten tenets:

1) one hundred-percent interoperability,

2) common operating environment,

3) flexible, modular C4I packages,

4) horizontal and vertical C2,

5) over-the-air updating,

---

138 Albert J. Edmonds. *C4I for the Warrior: Committed, Focused, and Needed*, June 12, 1993, The Joint Staff J-6.

139 Ibid.

6) warrior pull-on-demand,

7) real-time decision aiding,

8) global resource management and control,

9) adaptive safeguards, and

10) seamless operations.

These joint C4I tenets will be discussed in the context of the Army Enterprise Strategy.

Army Enterprise Strategy

Ten principles form the basis of the Army Enterprise Strategy[140] for exploiting current and future information technologies to enhance Army capabilities. These are

1) focus on the warfighter,

2) ensure joint interoperability,

3) capitalize on space-based assets,

4) digitize the battlefield,

5) modernize power projection platforms,

6) optimize the information technology environment,

7) implement multi-level security,

8) ensure spectrum supremacy,

9) acquire integrated systems using commercial technology, and

10) exploit modeling and simulation.

Together these ten principles represent a value-system that General Sullivan says leaders should use to make increasingly tough choices about information systems in a scarce resource

---

[140] Office of the Secretary of the Army, "The Army Enterprise Vision", 20 July 1993, Director of Information Systems for Command, Control, Communications, and Computers (C4), (Washington D.C.: The Pentagon, 20 July 1993).

environment. These tough choices will include, for example, which C4I systems to mark for elimination and what information technologies and C4I systems to invest in for the future.

Comparing the ten tenets of the Joint Staff's C4I for the Warrior vision with the ten principles of the Army's Enterprise strategy reveals, as expected, much overlap with some interesting differences. Two Army principles, ensure joint interoperability and optimize the information technology environment, map directly onto two joint tenets, 100% interoperability and common operating environment. One Army principle, digitize the battlefield, encompasses four joint tenets, horizontal and vertical C2, over-the-air updating, warrior pull-on-demand, and real-time decision aiding. This is so because digitization, tying together all the warriors and battlefield systems into an integrated digital information network, provides the means for the Army to achieve the four joint tenets. In the same way, adaptive safeguards, a joint tenet, encompasses two Army principles related to security of information systems, implement multi-level security and ensure spectrum supremacy. Despite these similarities, there are some notable differences.

There are two Joint C4I tenets, global resource management and control and seamless operations, that have no direct counterpart Army principle. Global resource management and control addresses the very important issues of managing and controlling C4I resources and infrastructure. How to monitor and control the performance of critical backbone services and connectivity to forces deployed worldwide is a major requirement. If the Army is just a user of this C4I infrastructure, then perhaps no management and control principle is needed in their vision. However, if there is Army-unique C4I infrastructure, then the Army should assess

how they plan to monitor and control the ability of that infrastructure to provide information services to Army forces.

The other Joint tenet without an Army counterpart is seamless operations. Seamless operations appears to focus on the functional needs of the warrior and the ability to conduct operations smoothly across diverse elements. For example, during the Persian Gulf conflict several Iraqi jets were able to escape to Iran because of the differences or seams that existed in providing a common air picture among Naval aviation, Marine ground-based air defense, Air Force interceptors, and Army ground based air defense. This tenet points to the need to erase all of those seams and those that might exist in other warfare areas. Although the Army's Enterprise strategy envisions seamless operations, it does not provide for a principle or a process to ensure them. For example, joint interoperability uses a certification process to try to assure that systems can actually interoperate. Perhaps by using live exercises or interactive simulations, operational seams could be identified and resolved across functional areas within the Army and across warfare areas of the services.

Conversely, there are four Army principles that have no direct counterpart Joint tenet. These Army principles are capitalize on space-based assets, modernize power projection platforms, acquire integrated systems using commercial technology, and exploit modeling and simulation. Two of these principles, capitalize on space-based assets and modernize power projection platforms, relate strongly to the Army's vision of split-based operations. In split-based operations Army installations in the US, power projection platforms[141], will provide continuous information, materiel, and maintenance support to deployed forces

---

[141] A power projection platform is the name the Army gives to installations in the US that are modernized to support the rapid deployment of forces anywhere in the world. These installations, such as Ft. Bragg, N.C., are closely tied to nearby airbases and ports to speed deployment.

overseas. Satellites provide the ability for deployed forces to exchange information with the bulky non-combat related computer systems such as personnel systems, logistics requests, finance records, and maintenance files and their associated operating personnel.

Several advantages accrue from this "hinge in space[142]." Demand for strategic lift is less since more people and equipment can stay behind and since only truly needed supplies and equipments are moved into theater. The time required for forces to enter and exit areas of operations is quickened. Since depot and other support activities may not have to deploy, combat service support can be uninterrupted and better sustained.

Another advantage of the "hinge in space" relates to the Army's concept of non-linear warfare in the 21st Century. This concept envisions widely dispersed enclaves of Army forces involved in swift maneuvers and standoff engagements. These enclaves are separated by distances beyond the range of terrestrial systems. Connectivity between these enclaves is provided by satellites which enables commanders to coordinate and support these widely dispersed forces.

There are two more Army principles without a joint tenet counterpart, acquire integrated systems using commercial technology and exploit modeling and simulation. Using commercial technology to acquire integrated systems is a statement of the Army's preference for using technology insertion and evolutionary advances over new system starts. Exploiting modeling and simulation describes the Army's vision of using state-of-the-art distributed simulation technologies for developing and testing rapid prototypes of new systems, training on current systems, and even for battle planning and rehearsals.

---

[142] The hinge in space refers to the communications connectivity provided by satellites to tie the warfighting forces deployed overseas with the support elements that remain in the US.

Deserving of special mention is the first Army Enterprise principle, focus on the warfighter. It contains five challenges to provide:

1) a responsive requirements process that reflects Warfighter needs;

2) soldier-friendly systems;

3) more deployable information systems;

4) capable and reliable systems; and

5) systems that function in both garrison and tactical environments.

Importantly, General Sullivan has created two processes to improve the requirements process and cope with the rapid advances in information technology. First he setup the Battle Labs process which provides a mechanism

> through which Warfighters and materiel developers can team with industry to explore new technologies and concepts. The Battle Labs testing process will have the added benefit of relating the cost of technology insertion to battlefield capability. We will know if the benefits on the battlefield justify the cost.[143]

Battle Labs can improve the requirements generation process because users will be exposed to new technologies and concepts and materiel developers will be better exposed to the user's warfighting needs. Promising technologies identified by the Battle Labs process can be inserted into existing systems. This technology insertion is another pay-off from the Battle Labs. Technology insertion applies new technologies to families of systems, such as armored fighting vehicles like M1 tanks and Bradley Infantry Fighting Vehicles, which must function together on the battlefield. For example, General Sullivan states "...we would insert technologies such as combat identification devices and advanced sensors by force package to provide enhanced capabilities for early-deploying forces"[144].

---

143 Ibid. 11.

The other process started by General Sullivan is the Louisiana Maneuvers which takes its name from pre-World War II large scale maneuvers in the state of Louisiana. This process involves a board of four-star general officers which reviews exercises, modeling and simulation results, wargames, and combat operation reports to identify warfighting issues that the Army must address. Part of the process involves the exposure of promising technologies to the highest levels of the Army. Armed with issues to solve and information technologies to leverage, Louisiana Maneuvers examines "the impact of changes in doctrine and materiel on the Warfighter in the field. Louisiana Maneuvers provides an unparalleled environment for identifying the Warfighter's information needs."[145]

Louisiana Maneuvers, really an initiative by General Sullivan to energize and guide the restructuring of the Army, is also examining and experimenting with high technology and conceptual changes in C4I. One of the major thrusts is to use modern computer communications technologies to create a high speed, high volume information network linking all major military installations and organizations[146]. This network will enable units and commanders at widely separated locations to train together in a virtual simulated battlefield environment. This distributed interactive simulation technology provides for realistic planning and rehearsal of future combat operations. What remains to be seen is whether these initiatives will be institutionalized in the Army and be carried forward by future Army Chiefs of Staff.

---

144 Gordon R. Sullivan and John W. Shannon, *Strategic Force- Decisive Victory: A Statement on the Posture of The United States Army Fiscal Year 1994*, March 1993.

145 Ibid. .

146 Gordon R. Sullivan and John W. Shannon, *Strategic Force- Decisive Victory: A Statement on the Posture of The United States Army Fiscal Year 1994*, March 1993.

The Army's oldest and still active C2 program is SIGMA STAR or the Army Tactical Command and Control System (ATCCS). It is very much a battlefield functional area approach. SIGMA Star refers to the five battlefield functional areas: maneuver, fire support, air defense, intelligence/electronic warfare and combat service support. For each of these areas there is a command-and-control system that is integrated by the overall system-of-systems, SIGMA STAR, an overarching architecture that integrates each area with the others and with other services as well[147]. Results from this effort have been mixed for two reasons. First, the acquisition bureaucracy causes long lead times and loses touch with operational realities. Second, operators, frustrated by the long lead times and difficult to use systems, have pursued independent solutions which can make integration and interoperability problems worse.

In the near future, ATCCS will transition to the most recent Army C4I initiative, Army Battle Command System (ABCS). This program envisions a seamless architecture[148] from the strategic level all the way down to the foxhole. In building ABCS, the Army places top priority on winning the information war. To succeed in winning the battlefield information war, "...the Army must have the capability to gather information, process it, transmit it around the battlefield, and deny any potential enemy the same capability."[149] To do this, the Army wants to digitize the battlefield. This digitization will improve "shared situational awareness" and "real-time force synchronization" by enabling rapid passing and display of enemy

---

147 R. J. Rechter et al., Army Tactical Command and Control Systems: An Integrated Approach, *Advanced Technology for Command and Control Systems Engineering*, ed. by Stephen J. Andriole, (Fairfax, VA: AFCEA International Press, November 1990), 439-451.

148 Seamless architecture is somewhat of a contradiction in terms. The essence of good architecture is the careful delineation of the seams or interfaces between subsystems. Hence, a seamless architecture means that the interfaces have all been carefully worked out so that the subsystems all operate smoothly together.

149 Gordon R. Sullivan and John W. Shannon, *Strategic Force- Decisive Victory: A Statement on the Posture of The United States Army Fiscal Year 1994*, March 1993.

information and friendly locations[150]. To make sure digitization happens in an integrated fashion across the force, the Army has recently created a Digitization Task Force to work the problems. Similar to the Army, the Navy has been working to use information technologies to improve C4I systems.

The Navy Sonata

The Navy's current C4I initiative is called Sonata because it is composed of three movements: Weltanschauung or "world view"; the Copernicus architecture; and the Croesus strategies. The first movement or "world view" refers to a new doctrine called Space and Electronic Warfare (SEW). SEW is the overall strategic objective of Sonata - "...to separate the enemy leader from his forces, to render the leader remote from his people,...and to control his use of the electromagnetic spectra[151]." Sonata's strategic objective is in concert with theory and operational experience. Theory recognizes that C2 is a two-sided contest, therefore targeting the enemy's C2 capabilities is logical. Operational experience in Grenada, Panama, and Desert Storm demonstrate the success of the SEW objective of "separating the leader from his forces". However, it may be that the Navy strategy needs more emphasis on developing friendly C2 capabilities. Sonata is really a command and control warfare (C2W) initiative.

The Copernicus movement is called a strategy for building a C4I system but it really is an "architecture" for information exchange. It consists of four pillars: the Global Information Exchange Systems (GLOBIXS), the Commander-in-Chief (CINC) Command Complex (CCC), the Tactical Data Information Exchange Systems (TADIXS) and the Tactical

---

150 Ibid.

151 Jerry O. Tuttle, *Sonata*, September, 1993.

Command Center (TCC). GLOBIXS and TADIXS are copper/fiber-based and radio-based computer telecommunication networks respectively.[152] They tie the CCC and TCC command facilities together into an interactive network of afloat tactical commanders, the CINCs, and the supporting shore establishment.[153] The architectural pillars are "...really [like] platforms - the electronic equivalent of ships, airplanes, and submarines" and have "clearly definable goals, production quotas, interfaces, and composition."[154]

The Croesus strategies describe how the Navy plans to go about "...fielding information systems technology in the midst of changing threat, exploding technology, and declining budgets."[155] Bottom line of the Croesus strategies is to transition from stove pipe programs to building block programs. There are three Croesus strategies for accomplishing this: Pyramidal Programming, Cyclical Production, and the Fleet Assembly Line.

Pyramidal programming is a classic application of an objectives hierarchy from systems engineering [156]. At the top is the strategic objective of SEW. Below the base are three tiers of subordinate objectives. The top tier is an architectural layer that describes SEW ends in more detail. The second tier is more a set of means to SEW ends. This tier is programmatic and contains program elements, appropriations and lines. The third and final tier is a set of technical means, "best-of-breed" building blocks of technological solutions, to accomplish programs which in turn support SEW ends.

---

152 According to Frank Snyder, the GLOBIXS and TADIXS are really distributed software networks and the CCCs and TCCs are centers of interoperable software packages. The interaction planned is between CCCs and TCCs -- not between TCCs.

153 Ibid.

154 Ibid.

155 Ibid.

156 Andrew P. Sage, *Systems Engineering*, (New York: John Wiley, 1992).

Cyclical production calls for careful attention to cost management across the entire life-cycle of building, buying, installing, operating and maintaining a system or group of systems. This philosophy recognizes that electronics and computing technology production should be impelled by not just operational requirements but also technology, budget, and support requirements. Advances in technology may present an opportunity, budget changes may drive programmatic requirements and the cost of maintaining old equipment may drive support requirements.

Fleet Assembly Line represents a way of thinking about how to put information technology products into the Fleet. The objectives of this approach are to make generational changes in concert with operational tempos and to conserve funding through "Just-In-Time" assembly.

Four implications of the Fleet Assembly Line approach are electronic platforms, modular installations on a grand scale, builder to shopper mentality shift, and programmatic flexibility. Electronic platforms means that GLOBIXS and other architectural components of Sonata will be platforms for the insertion of electronic building blocks of common hardware and software and unique-to-purpose application software. This approach will permit economies-of-scale as new ships or ships in overhaul receive modular electronic platform upgrades. The cultural shift in mentality from builder to shopper reflects the reality that many building blocks can be better obtained by leasing or buying information technology products and services from the commercial sector such as telecommunications leasing. The Fleet Assembly Line approach is very similar to the Army's concept of horizontal technical integration or technology insertion.

The Air Force Horizon

Horizon is the Air Force's overall strategy for modernizing its C4I capabilities. The strategy has four parts: the Air Force C4I Strategic Planning Process, the architecture planning process, the Air Force C4I Systems Master Plan, and the Communications Squadron 2000 initiative. The Air Force C4I Strategic Planning Process is "a disciplined process to develop and modify C4I capabilities" and "integrates the elements of Air Force C4I architecture development and migration planning to achieve an effective, interoperable and seamless C4I capability which supports joint, expeditionary operations."[157]

The architecture planning process examines four mission area architectures: combat, mobility, space operations, and special operations. Using these mission areas, the process applies common standards, components, and data definitions "in a consistent fashion to migrate existing legacy systems into a joint, interoperable, objective architecture."[158] The Air Force plans to use rigorous systems engineering techniques that employ advanced modeling and simulation technologies to develop the four mission area architectures. The Air Force C4I Systems Master Plan will reflect the results of the architecture planning process.

The C4I Systems Master Plan has both short-term and long-term goals and objectives. For the next Program Objective Memorandum (POM), short-term objectives include a "focus on C4I capability employment, and the associated communications connectivity, at fixed and deployed bases."[159] This short-term goal focuses on "building lightweight, user-friendly, transportable and highly reliable C4I capabilities."[160] Similar to the Army's vision, these C4I

---

157 Carl G. O'Berry, *Horizon: Air Force C4I Strategy for the 21st Century*, Air Force , (Washington, D.C: The Pentagon, Deputy Chief of Staff for Command, Control, Communications and Computers, Plans and Policy Division), 4.

158 Ibid, 5.

159 Ibid, 7.

capabilities that are used in garrison for daily operations and planning must be quickly deployable and operate the same way in the field as they do in garrison. The long-term goal is "the creation of a global C4I infosphere permitting each warfighter to view his or her part of the common air picture in real-time and transmit decisions for rapid execution."[161] The Air Force C4I Systems Master Plan will shape the systems which will provide these improved C4 capabilities. The backbone of Air Force C4I systems are its C4 support elements, the communications squadrons.

The Communications Squadron 2000 initiative puts modern technology to work to support expeditionary warfare by "organizing communications squadrons for identical forward- and home-based roles, enhancing wing capability for networking, and equipping communications units with lightweight, modular, interoperable systems."[162]

Ultimately, the Air Force Horizon Strategy envisions that "Combat air crews will come to rely increasingly on fused, near-real-time information depicting the battlespace from multimedia, global networks accessed, on demand, via deployable data terminals."[163]

Drawing on the theory, experience and technology observations previously discussed, there are both gaps and areas of strong agreement with the Star, Sonata and Warrior visions. First, the theory says the central part of any C4I system is the decision making that takes place. In this regard, the Joint Staff initiative receives praise for naming the vision after the decision maker to be supported -- the Warrior. Unfortunately, the vision does not define exactly who is the warrior and how many are there? All three initiatives can be criticized,

---

160 Ibid.
161 Ibid. 8.
162 Ibid. 11.
163 Ibid.

based on our theory, for not giving sufficient emphasis to the team concept. The team exists at all levels of war and all echelons of combat forces. For example, there is a joint team and the C4I visions of each of the services should describe how their visions relate to each other. Warriors are part of a team and their decisions necessarily impact the rest of their team. Therefore, they must have information that is relevant to their role in the team and information about the rest of their team. In other words, coordination is an important aspect in C2 and needs to be addressed more explicitly. Certainly a common tactical picture, an objective in all three visions, should help but is it enough? For example, what coordination mechanisms are we going to design into our systems? Even in Desert Storm we relied on couriers and liaison officers to effect coordination by delivering Air Tasking Orders or Operations Overlays. Although we can think of easy technology fixes to these courier missions, there may be unanticpated reasons, such as security, to maintain these older mechanisms.

Theory says that we should go beyond the idea of just a common tactical picture. We need our C4I systems to help us perform situation assessment. If the purpose of C2 is to recognize and respond to situations, then we need to evaluate C4I systems on their ability to do just that. Since situations have a time window-of-opportunity associated with them, we expect a C4I system to help warriors decide and act within the appropriate time constraints. The Navy's idea of a surveillance grid and a communications grid, making a visible representation of the electromagnetic spectrum over the battlespace, may be a very useful construct for understanding part of the C4I situation. But would we not also want to know if and when the enemy's C2 system has recognized an important situation? For example, has the enemy discovered the gap in our defenses? The Army's vision of "shared situational

awareness" seems to be closer to theory than the idea of a "common tactical picture". Operational experience from Desert Storm seems to validate the tremendous operational benefits from improved situational assessment.

There seems to be a gap in all three initiatives in terms of formulating and disseminating plans. Perhaps the emphasis on computer communications technology, interoperability, and seamless operations could or could not be interpreted as supporting planning. It is important to remember that C4I systems should support planning. The Army's Louisiana Maneuvers initiative includes some support for planning and rehearsals which merits attention. Execute and monitor combat operations is another function of C2 from our theoretical discussions that seems adequately reflected in all three initiatives by their emphasis on generating the common tactical picture.

The Navy's Sonata initiative incorporates the idea, reinforced by operational experience in Grenada, Panama, and the Persian Gulf, that C2 is a two-sided contest. SEW's objective of separating the enemy commander from his forces and people has proven merit. More emphasis on the development of friendly C2 capabilities is perhaps needed in the Sonata vision. The "friendly" equivalent of the focus on the enemy commander in SEW is really a set of defensive measures that permit continued functioning of freindly C2 once an enemy decides to attack or subvert it.

Operational experience shows that we are increasingly relying on space-based communications especially at the Joint Task Force level and above. The possibilities of interception or interruption of such communications should not be overlooked. The Johnny Walker spy case is an example to remember. The great range and connectivity afforded by

such communications also raises the level-of-control issue that surfaced in Vietnam operations.

Information technology promises much especially as computer hardware becomes smaller, cheaper yet faster, and with more and more storage capacity. This means computers will be proliferated in many more mobile configurations. A challenge is to understand how to allocate tasks between people and computers. Also, what, if any, back-up manual training or systems are needed? Computer software is moving toward a common "look and feel" user interface. Also, many hardware compatibility and interoperability problems can be addressed by software solutions. Commercial investments and applications in information technology will provide much leverage to C4I modernization efforts. The Navy recognizes in Sonata the importance of shifting from a buyer to a smart shopper.

The major disconnect in all of the C4I visions, DOD, the Joint Staff, and the Armed Services is that there is not a unifying C4I framework on which to hang all of the good "buzz words" found in the various visions. There needs to be a definition of military command and control, an explanation of the command and control process, and an explanation of how C4I systems support both in the visions. For example, if command and control is all about making decisions related to recognizing and understanding situations, developing and disseminating plans, and directing and monitoring combat operations, then the visions need to say so and explain how their initiatives will improve situation assessment, planning, and operations. In other words, the visions mainly say what they need but do a poor job of explaining why they need it. Understanding why something is needed is important because it provides the basis for setting priorities and measuring progress.

CHAPTER VIII

CONCLUSIONS AND RECOMMENDATIONS

This section summarizes the disconnects that cause major difficulties in designing, testing, and using C4I systems and what is being, or can be done about them. Promising future directions for C4I systems and what these directions mean in terms of changing C2 processes and warfare in general are discussed.

C4I System Building

The table below summarizes the main disconnects discussed in this research that cause difficulties in designing, testing, and using C4I systems. The second column presents the primary effect of each disconnect while the third column lists promising initiatives[164] that may help resolve the disconnect and mitigate the effects.

Scope	Disconnect	Effect	Initiative
DOD	Rapid advances in the underlying technologies.	Systems fielded with obsolete technology.	DMRD 918, C4IFTW, Army Enterprise, Navy Sonata, and Air Force Horizon.
DOD	Burdensome and lengthy acquisition process.	Costly, duplicative legacy systems.	C2 Migration
DOD	No process exists for determining or managing change to C4I systems.	Many symptomatic fixes but no institutional or organizational changes.	None.

164 Only initiatives known to the author are listed. There may be others, of course.

Scope	Disconnect	Effect	Initiative
Joint	Services develop separate stovepipe systems for command and operation centers, communications, and intelligence.	Systems that do not interoperate in a joint warfare environment.	C4IFTW CJCSI 6212.01
Service	Within each service, functional areas develop separate systems.	Systems that do not interoperate across functional areas.	Army ATCCS (ABCS); Air Force Communications Squadron 2000
Design	User requirements lag technology and are unstable and ill-defined.	Systems do not meet the effective needs of the user.	Army Battle Labs; Air Force C4I Strategic Planning Process
Design	No common understanding of C4I architecture.	No threads of continuity across designs.	DOD's Technical Reference Model and Standards Profile.
Design	Lack of well known and accepted standards.		DOD's Technical Reference Model and Standards Profile.
Design	No consistent approach to automation and human-machine interaction for C4I.	Costly errors during actual combat operations.	None.
Test	Degradation in interoperability during development.	Systems deliver less interoperability than planned.	CJCSI 6212.01
Test	Evaluation of legacy systems.	Existing systems remain in operation beyond their usefulness.	Written guidance from ASD (C3I) and DISA.

Scope	Disconnect	Effect	Initiative
Test	Ad hoc integrators	Systems are not robust and are difficult to maintain.	None.
Test	No accepted metrics for C4I systems.	Difficult to evaluate the value-added of investments in C4I systems.	None.
User	Many different vintages, generations, and versions of C4I systems and equipments.	Incompatible systems require many workarounds in the field.	None.
User	Systems lack functionality. They sometimes cannot do what the user wants them to do.	User is frustrated.	None.
User	Systems are not easy to use. Although they can do what the user wants, the user finds it too difficult to operate.	Users revert to manual procedures and the system is not used.	None.
User	User interfaces do not support thinking in warfighter terms.	Users find the systems less useful than they could be.	None.
Design, Test, User	Lack of common language and understanding of C4I systems.	Communication difficulties exacerbate other disconnects.	None.

Although there are many initiatives in place to account for the rapid advances in the information technologies underlying C4I systems, there is not much evidence to suggest that a

process has been established and institutionalized to manage that change. Even if all the visions of the Joint Staff and the Services lead to well-thought-out implementation plans, these plans could become quickly outdated as technology continues to advance. When the current high-level emphasis on migration systems subsides, after most of the savings have been mined out of consolidation, where are the processes in place to continue to deal with legacy systems? From a life-cycle systems management perspective, every C4I system, like any other system, will eventually have to be retired. Therefore, legacy systems will always be a fact of life and a management perspective that plans for this fact will have a better chance for success.

Joint Staff initiatives seem to be making good progress towards interoperability by putting in place a process that requires interoperability certification, compatibility testing, standards coompliance, and security accreditation. Still, the development of C4I systems is not accomplished using a "system of systems" viewpoint. Too often, communications or intelligence officials of the individual services are put in charge of C4I development. Although their technical background is very relevant to C4I, their narrow functional perspective can mislead C4I programs. If C4I is truly for the warrior, then warriors should be driving requirements from a "system of systems" perspective. Without a strong warfighter in charge of C4I systems, the many small programs that together add up to the C4I capabilities of US forces will be less effective than they otherwise could be. In this sense, the communications systems, intelligence systems, computer systems, and military command and operations centers and facilities should all be integrated into a coherent C4I system within and across every echelon and service before an operation begins. Field assembly on-the-spot by

the senior commander is not a good way to do business. The services need to get past dumping all of these individual pieces of C4I systems and equipments in a CINCs lap and expecting the CINC to put it together under the stress of crises or combat.

Better designs are needed and obstacles that prevent such designs can best be removed by education. For example, since the commercial sector is really driving information technology, if C4I requirements are to reflect the warfighter's needs and take advantage of state-of-the-art technologies, then the services need to get inside the commercial information technology world. We need technology scouts, experienced warfighters with some training in technology assessment, to live and work with the commercial sector as a way to transfer knowledge to the C4I development process.

Requirements engineering is really a sub-specialty of systems engineering. The services need systems engineers who have been formally educated in systems engineering methodology and systems engineering processes. These engineers can provide the interface needed between the warfighters and the technicians in order to negotiate between warfighter needs and technical capabilities in order to produce valid requirements. Legacy engineers who are trained in only a narrow discipline need to be taken out of systems engineering roles and transferred to detailed technical design efforts more appropriate to their background. In this regard, systems engineers who have graduate work in C4I relevant areas of study are especially needed.

Education of all military officers should include formal study of command-and-control and C4I systems. This will help develop a common understanding of C4I across the force. This study could be integrated into existing curriculums that study military operations.

Increasingly, the role of officers in war will be focused on the battle for information and what better way to prepare for that battle than a thorough understanding of the means for winning it: the command and control process and the C4I systems that support it. This does not imply that warriors must be immersed in technical C4I knowledge or jargon. Instead, commanders and warriors need an operational knowledge of military command and control with an understanding of how people, the command and control process, and C4I systems interact. This should give military leaders the knowledge needed to make better decisions about positioning and operating military forces and help to identify and correct human, process, and system errors. For military and civilian officials serving in positions that manage C4I systems, short courses should be developed to get everyone to where they can have a common understanding and language for grappling with relevant C4I issues such as standard architecture.

Standards can be a powerful tool in design but they can also prove to be a hindrance. A process to continually re-evaluate the costs and benefits of C4I standards needs to be put in place. This needs to be an independent, honest process as free from the influence of stakeholders of existing standards and legacy systems as possible.

Designers need to include provisions for making their C4I systems easier to test. For example, designers can put in devices that record all the human interactions with a system and system-initiated events to provide an accurate representation of both live and simulated operations similar to flight recorders. In the interim, testing can be improved by using commercial facilities and practices. For example, for software applications, a two-step alpha and beta user test is normally practiced. These tests involve many actual end-users

experimenting with the prototype or early release versions of the application in the end-users' environment. Many problems are identified and corrected by the feedback received from this process. In the commercial sector, information technology products and services often undergo extensive testing in usability centers. These centers identify many system problems such as human-machine interaction difficulties and functionality shortfalls. A usability center with advanced modeling and simulation technologies could test systems that are still in the virtual prototype stage.

Testing C4I systems needs to synchronize with how these systems are developed. If incremental, evolutionary development takes place, then testing needs to proceed in a similar fashion. For example, C4I system architectures, when properly defined, can be computerized and tested usually before any equipment has been networked together. Metrics for testing C4I systems need to focus on the functionality and usability aspects of the system. In other words, does the system do what the warfighter wants it to do and is it easy enough for the warfighter to get the system to actually do it? Is this system supporting decision making related to situation assessment, planning, and conducting operations? How does this system support the command-and-control process? Does the system help the warfighter make quicker situation assessments, better plans, and conduct more effective operations? Does the system support thinking in the warfighter's terms? These are all questions that tests must answer since they all relate to the basic purpose of command and control, to support the warfighter's decision making requirements.

Testing should also prove that the system will work well in the existing and future environment. This means that tests ought to determine if the new system will work well with

existing systems and can the new system be easily adapted to work well with future systems. Once again, systems architects who understand systems integration should be representing the warfighter to the materiel developer. Testing ought to use a life-cycle approach that ensures interoperability certification, standards testing ,and security accreditation are achieved and maintained. The testing process itself should be evaluated to ensure that the expensive and time consuming activities of testing achieves benefits that justify their cost.[165]

Users will be spared from many difficulties with C4I systems if testing is incrementally accomplished. Finding problems early in the life of a system minimizes the cost of correcting them and reduces the number of users that are subjected to problematic systems. Still budgetary constraints and combined or coalition warfare will probably always put the warfighter in a difficult environment where many versions and vintages of C4I systems and equipment exist. Only by accepting this situation as the norm and building systems that can accommodate change both forward and backward will real progress be made. Even as we pursue tomorrow's objective of self-configurable, plug-and-play architectures, we must plan on providing the warfighters the translators, converters, and adapters they need to put C4I systems together today.

In summary, the most important point to make for C4I system building is that *success depends on managing change*.[166] Managing change requires a *process for determining what*

---

165 Andrew P. Sage, Systems Engineering, John Wiley New York, 1992, 161.

166 This call for managing change should not be interpreted as a desire to build a bigger bureaucracy for C4I systems. The last thing C4I systems need is a body of officials and administrators in a large hierarchy with fixed routines and lots of red tape. There is no way that such a bureaucratic approach can keep up with the rapid pace of change in the underlying information technologies. Smaller, flatter organizations with clear lines of authority to an overall decision maker are needed in the government staffed by educated and experienced officials who are networked with systems engineering research and development firms expert in C4I; with centers of excellence for C4I in academia; and with commercial designers and developers of C4I systems.

changes are needed.[167] The philosophy that guides those in charge of building C4I systems should reflect the ideas in this definition of configuration management:

> Configuration management is the systems management process that identifies needed functional characteristics of systems early in the life cycle, controls changes to those characteristics in a planned manner, and documents system changes and implementation status. Determination and documentation of who made what changes, why the changes were made, and when the changes were made, are the functional products of configuration management.[168]

Note that *determining change* as well as documenting change is important. We need *better mechanisms for determining change* for C4I systems. These mechanisms should blend technology forecasting and assessment, and technology transfer constructs with warfighting needs so that the forces of technology push and warfighting pull are considered together. Insights about how to adapt existing warfighting doctrine and organizations and how to design new doctrine and organizations to take best advantage of new technologies should be possible from such efforts as suggested here.

The research discovered eighteen major disconnects. First, many difficulties stem from the rapid advances in the underlying information technologies. Although the Department of Defense (DOD) used to drive these advances, they are now clearly driven by the commercial, non-defense sector. DOD, the Joint Staff, and the Services have a number of promising initiatives underway. Resolving this disconnect requires two important ingredients. First, a *process* needs to be established and continually improved to *manage change*. Part of this process must have *mechanisms to get inside the commercial development world of information technology* or DOD will increasingly "be on the outside looking in."

---

[167] A process is a series of progressive and interdependent steps for accomplishing some end that is applied continuously. This means, for example, that while step two is being done now, there is also a new step one being done that will lead to a new and better step two.

[168] Andrew P. Sage, Systems Engineering, New York: John Wiley 1992, 137.

Complicating the first disconnect is the burdensome and lengthy acquisition process. This disconnect makes C4I systems more costly than needed and often the systems are quickly out-of-date, old and undesirable, especially when compared to the commercial world. These *legacy systems* are difficult to use and maintain. Efforts to migrate legacy systems need to be accomplished. However, no "one time fix to the problem" will suffice. Since all systems progress through a lifecycle, they will all, at some point, need to be retired or evolved into a new system. Hence, every system may, at some point, become a legacy system or require a plan to evolve it to a new one. Again, a *process to continually manage the evolution or discontinuation of legacy systems* is needed. Reforms to the acquisition process are also needed. Reforms that embrace *incremental, evolutionary development* and allow for *a closer partnership between DOD and the commercial sector* are overdue. Incremental development cannot happen unless DOD can work closely with the commercial sector. This is a very tough problem since resolution probably requires legal and legislative changes.

Historically, the Services have developed separate "stovepipe" systems for command and operations centers, communications systems , and intelligence systems. Difficulties with interoperating these "stovepipe" systems in a joint warfare environment are well known. The Joint Staff addresses this disconnect by requiring interoperability certification, compatibility testing, standards compliance, and security accreditation for new systems and older systems being improved. Although these initiatives are very helpful, they tend to be a symptomatic treatment. A *"system of systems"*[169] approach headed by a senior warfighter needs to replace the hold that the communications and intelligence communities have on C4I.

---

[169] A "system of systems" approach would look at communications systems, command and operations centers, and intelligence systems as *components* of a larger C4I system. It would consider how these components work together to support the decision making that takes place to position and operate military

Within each service, there are many functional areas that all have legitimate C4I needs. Still these needs must be addressed in an integrated, disciplined way. This disconnect can cause the same information to get collected twice or not to be available to those with a legitimate need. Each service must have a "system of systems" approach to C4I that coordinates across functional areas within their service and across warfare areas with other services. Again, a senior warfighter is the right leader for shaping a service's C4I systems. Although the communications and intelligence specialties have much to contribute to C4I systems, the systems need to focus on the warfighter.

The definition of successful design is meeting the effective needs of the user. In C4I systems, users are the commanders and warfighters. This means the front-end of the design process, specifying user requirements, is very important. Unfortunately, because of the meager resources applied to the requirements end, user requirements lag technology and are unstable and ill-defined. As a result, systems are fielded that do not meet the effective needs of the user. Systems engineers, representing the user, need to provide an interface between the warfighter and the detailed design engineers to ensure that valid requirements are generated. Designs of C4I systems must be entrusted to those who understand systems engineering methodologies and processes. A common understanding of C4I architecture needs to be spread through the C4I community so people can talk to each other intelligently. Promising methods are available now for understanding and modeling the functional, physical, and operational architecture of C4I systems. The services should take advantage of this

---

forces. Careful attention would be paid to how the various components relate to each other -- how they interact in performing the various functions necessary to support the command and control process. A detailed understanding of how the components help commanders recognize and understand situations, formulate and disseminate plans, and direct and execute combat operations would be pursued.

technology so they can analyze the performance of architectures before any networks and nodes are installed and operated.

The final and perhaps most tragic disconnect in design is that there is no consistent approach to automation and human-machine interaction for C4I systems. The result is often the unintentional loss of human life during operations due to fratricide or other unintentional errors. Information technology and human-machine systems design research offers many promising approaches. An understanding of the human, process, and system interactions and error modes must be achieved and worked in interactive, virtual environments before C4I systems are actually built and deployed.

Testing and evaluation of C4I systems suffer from a lack of metrics and an ad hoc approach to system integration. As a result, it is difficult to evaluate the value-added of investments in C4I systems. Also, existing systems remain in operation beyond their useful life because they are rarely re-evaluated. Systems are not robust and are difficult to maintain once the "ad hoc integrators" that put the project together move on to another contract. Resolving these difficulties requires that legacy integrators be replaced by true systems integrators. System architects need to incorporate into their system design considerations of legacy systems as well as replacement systems. Importantly, rapid prototyping of C4I systems with a "build a little, test a little" approach is desirable. Testing should focus on functionality and usability. Can the system do what the user wants it to do and is it easy for the user to get the system to do it?

Many disconnects filter down to the user. As mentioned, systems often lack true functionality. They simply cannot do what the user wants and needs them to do. Sometimes,

even though the functionality is there, the systems are too difficult to operate. The user interfaces, the displays and controls used to operate systems, often do not support thinking in warfighter terms. The result is that users sometimes revert to manual procedures and find systems less useful than they could be. Better designs and testing should overcome some of these obstacles. Usability centers that simulate involve real users in simulated operational environments can identify and help correct many of these problems. Most importantly, C4I systems must be adaptable to the operational realities of the users' warfare environments. This means that prototyping in the user's environment is crucial.

Changes to C2 Processes

How will the command and control process of recognizing and understanding situations, formulating and disseminating plans, and executing and monitoring combat operations, be affected by advances in C4I systems? In terms of situation assessment, there will probably be significantly less human effort devoted to recognizing and understanding the current situation. Why? Because inexpensive sensors combined with wireless communication technology will be able to record and transmit all of the status reports and situation reports that now require human effort. Moreover, the compilation of all this information into an understandable situation picture will be enhanced by information fusion, display, and multi-media technologies. If the newer C4I systems are successful, this will give warfighters the ability to recognize and understand situations much earlier in the time window of opportunity. Hence, planning and disseminating orders will be accomplished more quickly. Plans will improve since computers will be allocated the routine tasks of keeping track of many of the details, thereby freeing people to concentrate more effort on creative work.

Plans will also improve because simulation and animation technologies will permit planners to test out their ideas in virtual environments that can represent key operational realities. With computer support, more options and contingencies can be explored. Further, video teleconferencing and distributed simulation will permit the involvement of lower echelon key personnel in the process. Those charged with executing operations may have a stronger voice in higher level planning. Dissemination of plans will be electronically done with plans communicated at light speed in multi-media formats so that subordinate elements can unambiguously grasp the operational intent of higher level commanders and rehearse their role in the operation.

Since planning will be accomplished better and quicker, operations can begin earlier in the time window of opportunity. Therefore more human effort will be freed to concentrate on predicting future situations and building future plans. Execution and monitoring of operations, largely a supervision process, will become more automated with higher level command and operations centers only intervening when alerted to deviations from the intended concept of the operation by system prompts. Coordination of many of the detailed aspects of an operation, such as supporting fires, will be pre-planned and launched automatically when software processes, running in the background, are triggered by meeting certain conditions. This means there will be much more emphasis on what a commander wants the force to do in the future instead of what they are doing now. This pull of the commander into the future may mitigate against the fear of over centralization of current operations.

How are these changes in the process going to affect C2 organizations? Organizations will become flatter and command and operations centers smaller and more distributed. Many of the routine, bookkeeping functions performed by today's echelons will be automated and consolidated in higher level echelons. Similar to what has happened to business, so called middle managers involved in administrative functions will become redundant and can be eliminated. For example, McDonald's no longer needs a multi-level bureaucracy to collect and monitor sales. Now, within seconds, the national office knows that you have just ordered a hamburger and that one hamburger order becomes a part of national, regional, and local buying patterns that can be continuously displayed and analyzed to improve current and future sales.

Connectivity, which will be possible from the National Command Authority to the individual soldier, sailor, marine, and airman, will create a tendency to centralize the command and control process. However, this tendency to centralization will be mitigated by two factors. First, the pull to the future as previously mentioned and the ability to consider more interactions at every level of command. For example, it will be much more apparent that there are very strong interactions among the political, economic, and military aspects of national power. Although the NCA will recognize their ability to become fascinated with lower level operations, they will come to realize the much greater impact their efforts could have by better coordination among the three elements of national power. Likewise, at every echelon, the ability to improve coordination laterally may properly preclude commanders from over supervision of subordinate echelons.

Changes to War

Many argue that the very nature of warfare is changing rapidly due to the advances in information technology. The affect that the information age is having on warfare is compared to the changes caused by the agrarian revolution and then the industrial revolution. In fact, several new terms are emerging to describe this revolution in military affairs such as information war or knowledge warfare. According to some observers, a revolution in military affairs

> occurs when the application of new technologies into military systems combines with innovative operational concepts and organizational adaptation to fundamentally change the character and conduct of conflict by producing a dramatic increase in the military effectiveness of armed forces.[170]

Applying this notion to American armed forces, several main evolutions are usually described. First, railroads, telegraphs, rifled musket and artillery transformed the Civil War battlefields from "those of the American revolution to ones presaging World War I."[171] Next, the internal combustion engine, radio and radar, and aviation technology caused major changes to warfare from World War I to World War II. Now the computer, the microprocessor, information, communications and space technologies are changing warfare again. These three types of warfare are compared to the civilian advances in the agricultural, industrial, and now information revolution to show how there is another revolution in military affairs taking place now. While I believe this to be true, I do not agree with the popular assumption that follows which asserts that the basic nature of warfare is changing.

In my opinion, there has long been three basic parts to warfare: maneuver, firepower, and information. Advances in maneuver can be categorized by their effect on the level of war,

---

170 Harry K. Lesser Jr.. The Revolution in Military Affairs and Its Effect on the Future Army, Advanced Research Department. College of Naval Warfare. Newport. Rhode Island. 2.

171 Ibid.

strategic, operational, and tactical. Firepower, historically killing power, has come to have three aspects: range, lethality, and accuracy. Information, the commanders and warriors historic need to see and understand the battle, subdivides into the functions of gathering, processing, storing, displaying, and transmitting information. Examining the technological advances leading up to World War I, we see that most of the gain occurred in firepower, rifles, artillery, and machineguns. The range, accuracy, and lethality of firepower was tremendously improved by the technological advances before World War I. In the naval forces, the preeminence of the battleship testifies to the dominance of firepower even in maritime strategic thinking.

The railroad was the primary advance in maneuver but it really only effected strategic mobility. We could now get lots more people, equipment, and supplies into the firepower killing fields of World War I. The only information advance, the telegraph and then later the telephone, was limited because it was relatively immobile and relied on fixed sites and wire which were both vulnerable to firepower. Therefore World War I can be characterized as firepower warfare with high attrition as an expected outcome.

If firepower characterizes advances in warfare through World War I, then maneuver characterizes warfare since then. The internal combustion engine and the aircraft made possible the development of weapons platforms with the necessary operational and tactical mobility to break the stalemate that firepower held on battle. New platforms to enhance mobility were developed. The aircraft carrier combined two platforms, the ship and the aircraft, to achieve maneuver capabilities with strategic, operational, and tactical implications. It is important to note how new combinations of capabilities and technologies can make for

significant improvements in military effectiveness. The tank and the submarine were improved to be platforms with immense capabilities to maneuver, receive information, and deliver firepower.

Radio and radar were two very important information related advances that not only improved the ability of military forces to gather and exchange information, they also greatly enabled the improvements in mobility by helping commanders position and operate military forces on the move. Still, the dominant characteristic of warfare was maneuver which was carried out by more and more capable platforms of war.

Now, as one assesses important technological advances of today and those forecast in the future, it is clear that the advances which will dominate our thinking about warfare will focus on information technologies. Stand-off weapons platforms, smart weapons, and precision-guided munitions all depend on information for their military usefulness. True, the development of nuclear weapons and associated delivery capabilities somewhat degraded the importance of certain information since "close enough was good enough." But, the undeniable need to protect our forces from weapons of mass destruction has actually increased the importance of quickly finding and using the right information. Therefore, the third wave of warfare, information age warfare, is totally appropriate. However, the basic nature of warfare is not changing. Warfare has always had the three components of maneuver, firepower, and information. For example, Sun Tzu's work several thousand years ago has many references about the importance of information. For example, he writes,

> By altering his arrangements and changing his plans, the skillful general keeps the enemy without definite knowledge. By shifting his camp and taking circuitous routes, he prevents the enemy from anticipating his purpose.[172]...What enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the

[172] Sun Tzu, *The Art of War*, edited by James Clavell, (New York: Delacorte Press, 1983), 65.

> reach of ordinary men, is foreknowledge.[173] ...If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.[174]

What continues to change in warfare is not the basic nature of warfare but instead the technological advances that make it possible to make more advances in one aspect or another of warfare. In other words, it is the means to carry out warfare that changes not its basic nature. If the underlying nature of warfare was truly changing then the study of the history of warfare would be sheer folly. We know that many valuable lessons about warfare can be learned from history. And as some have pointed out, one thing we learn is that nations in the past have taken different approaches to how best to take advantage of new technologies for the conduct of war. The winners are those armed forces that develop appropriate operational concepts and make the organizational changes necessary to get the maximum military effectiveness from new technologies in military systems.[175]

There are several important questions from a command and control perspective. First, are the military forces or operations that commanders and warfighters control going to be so different that changes in the C2 process or C4I systems need to be considered? Is the nature of modern warfare operations changing so significantly that we need to adjust doctrine, force structure, operations, and training?

Information technologies, stand-off weapons platforms, precision guided munitions, and smart missiles will blur the distinction between the strategic, operational, and tactical levels of war mainly because communications technologies and stand-off weapons will increasingly make every location on the globe seem equidistant from every other location.

---

173 Ibid. p. 77.

174 Ibid. p. 18.

175 Lesser, Revolution in Military Affairs, 7.

Also blurred will be the distinction between peace and war since the opportunities and vulnerabilities for engaging opponents with information technology resources will be so lucrative or so potentially damaging that constant vigilance will be required to serve and protect the nation. Information technologies provide opportunities to engage an adversary's information resources, manage the perceptions of their leaders, confuse their population, and mislead their armed forces. However, the globalization of information technologies makes all nations potentially subject to these vulnerabilities. Although a distinction may be drawn between information-based warfare, which may be ongoing at all times, and command and control warfare (C2W), which tries to destroy and disrupt enemy C2 capabilities while protecting friendly C2, both will be ongoing continuously. Only the decision making authority and the scope of the operations will distinguish them. As a result, systems to monitor and control information resources and C4I systems are needed.

Even though the basic nature of warfare may not change in terms of the basic objectives of war, the means to accomplish war, the number of functions that a commander must coordinate and the number of different types of weapon systems involved, continue to be more complex. Doctrine needs to accommodate these changes and emphasize winning the information war. Force structures need to account for the increased importance of the information dimension of warfare. Organizations and staffs should be able to be made flatter and smaller respectively by using information technology to accomplish many routine and burdensome tasks. Training and education need to integrate formal classes on command-and -control and C4I systems. This does not mean that warriors need to be immersed in technical C4I knowledge or jargon. Instead, commanders and warfighters need an operational

knowledge of C4I systems with an understanding of how people, the command and control process, and C4I systems work together to win information operations, prosecute C2 warfare, and accomplish command and control. But winning requires more than knowledge as Sun Tzu warns, "One may *know* how to conquer without being able to *do* it."[176]

Although, this warfare system point of view argues that the basic nature of war has not changed, the other side of the argument is that new technologies now provide the means to accomplish war in better and different ways. For example, in Sun Tzu's time, the two basic ways to accomplish deception were to manipulate spies with false information and to maneuver forces in circuitous directions. With advanced information technologies, it may now be possible to accomplish deception by inserting false information into the enemy's civilian and military information systems. These new ways of accomplishing long standing warfare functions, have led many to say that there is a revolution in military affairs. One of the main parts of this revolution is called information warfare.

There are three schools of thought that seem prevalent in the current debate about information warfare. One school of thinkers, call them "publicists", believes that open disclosure of information about conflicts will lead nations and groups to take actions to limit and resolve conflicts without resorting to military force. Should military conflict occur, the publicists believe that wide dissemination of the horrors of such military contests will quickly bring an end to them. In contrast to the publicists view, another school of thought, call them "selectivists", thinks that information is another tool or resource of war so it should be guarded, used and released selectively to accomplish specific purposes. The final school of thought, call them "traditionalists", are very wary of investments for waging war that do not

---

176 Sun Tzu, *The Art of War*, edited by James Clavell, (New York: Delacorte Press, 1983), 19.

achieve violent effects. The traditionalists believe, if C4I systems are really just information systems oriented to support warfare, that once war is chosen as the way to achieve policy, then violence is the best way to exercise power to impose one's will on an enemy. These different schools of thought about information warfare may have considerable impact on future systems. So which school of thought is correct?

As with many parochial views, the real answer is often a combination of the different viewpoints and this case is no exception. For example, the publicists are right that sharing information about conflict may cause nations and groups to limit that conflict. However, the publicists should not reject the very other real possibility that knowledge about a conflict may catalyze nations and groups to participate on one side or the other of a conflict. This means that the horrors of war may stimulate and enrage people to violence as much as it may encourage others to peace. This is one of the great unknowns of war cited by Clausewitz when he warns that wars, due to human emotions, may quickly escalate beyond control. Further, extensive worldwide coverage of conflict by CNN seems to have met with very mixed results. It is not at all clear whether wide coverage widens a conflict or narrows it. Still, whether one agrees with the publicists or not, media coverage and as-it-happens information about future conflicts is likely to continue to grow. Even soldiers and sailors in the future may have access to personal wireless communication technology that allows them to video teleconference with Mom back home via future satellite systems such as Motorola's Iridium and the Gates/McCaw Cellular's Teledesic. It is reported that some commercial research labs are developing Unmanned Aerial Vehicles, not for military use, but for civilian uses such as remote news coverage and remote tourism by broadcasting live images. So it

may be increasingly difficult for military authorities to control information about conflict. Despite the difficulty of doing so, it may still be desirable to establish control over military conflict information flow. If so, then C4I systems that can accomplish this need to be designed and soon.

In addition to the information control problem, some argue that selectivists will encounter other difficulties. As Thomas Jefferson said, "Information is the stock of democracy." Because this belief in the value of information to the functioning of democracy is strongly held, there will always be constraints on what can rightfully be withheld from the American people. In addition, some information channels may be untouchable by military authorities due to the concern for protecting the privacy of American citizens. Technology itself may make it much more difficult for the government to intrude on private information channels.[177] Hence, there will always be a balance that needs to be struck between freedom of information and national security needs. Should enemy nations or groups acquire the ability to penetrate and manipulate civilian information channels in the US, then government authorities may be decide to become more involved in securing these channels from enemy exploitation. C4I systems that can monitor these channels and help control and execute operations to restore them to normal would then become legitimate national security needs. At the same time, checks and balances need to established to ensure that power over information channels is not abused.

---

[177] For example, a computer scientist at AT&T Bell Laboratories, Dr. Matthew Blaze, recently discovered a flaw in the US Government's Clipper technology which was to be used to let law enforcement officials wiretap encoded telephone calls and computer transmissions. Apparently, Blaze found a not-too-difficult way that to use the Clipper chip itself to encode messages so that even the US Government could not unscramble them. Also, Blaze disclosed this information with many other scientists and researchers who discussed the matter world wide over the Internet. See John Markoff, "At AT&T, No Joy on Clipper Flaw," *New York Times*, 3 June 1994, D2.

We need to remember that warfare is multi-dimensional and that we should not ignore the firepower and maneuver aspects of warfare in favor of information-based warfare alone. But, the technological advances of our time demand that we pay more attention now to how best to take advantage of the new information technologies. We need to determine what innovative operational concepts and what organizational changes will have the highest payoff in military effectiveness for future conflicts.

There are some dangers to avoid as we pursue these questions. Since war is two-sided, there are many uncertainties that our opponents largely control. Using advances in information technologies as a simple excuse for mining more dollars out of the defense budget is a dangerous course of action. This does not mean we cannot find real savings by judiciously applying information technologies. It does mean that we must not shrink so small that our forces are vulnerable to a technological surprise or pre-emptive attack because we assume we will know about both with ample warning time. Size is still an important factor in the ability of an armed force to absorb aggression.

APPENDIX A

STRUCTURED INTERVIEW QUESTIONS

1. Identification
   - Name
   - Organization
   - Position

2. This research investigates **what causes the disconnect between designers, testers, and users of military command, control, communications, computers and intelligence (C4I) systems and what can be done about it**. Which of these three communities best describes your experience with command and control systems?

   - Design and Development
   - Test and Evaluation
   - Military User or User Representative
   - Other

3. C4I systems are often *classified according to the levels of war*. Which level of war best describes your experience with C4I systems?

   - Strategic - NCA (Nuclear)
   - Operational - Joint (Conventional)
   - Tactical - Service Components

4. C4I systems are often *tailored to support specific warfare environments*? Which warfare environment best describes your experience with C4I systems?

   - Air
   - Land
   - Sea
   - Space
   - Special Operations

5. C4I systems are often *tailored to conform to service cultures and norms*. Which service best describes your experience with C4I systems?

Air Force
Army
Navy
Marine Corps
Other

6. The next several questions attempt to capture your perspective on command, control, communication, computers, and intelligence (C4I) systems. **Some researchers contend that C4I systems are not really designed and fielded. Instead we field three separate systems, a telecommunications system, command centers, and intelligence systems.** If you agree with this statement, which of these three systems best describes your experience? If you disagree, please describe how you do or do not partition C4I and where your experience lies? Please cite specific examples?

Agree
- Telecommunications Systems
- Command Centers
- Intelligence Systems
- Example

Disagree
- Example

7. As you know there are many acronyms associated with command and control. Some researchers explain command and control (C2) as the process that commanders use to exercise the function and responsibility of command over assigned forces. Command emphasizes the commander's role of decision making in coordination with other echelons to position and operate military forces while control brings in the role of the staff in providing and disseminating information in support of the commander. C3, C4, and C4I are terms that refer to the systems and enabling technologies that support the commander's decision making and the staff's information requirements. If you agree with this assertion, which aspect of command and control relates best to your experience? If you disagree, please explain your view of command and control and your area of experience. Please cite specific examples.

Agree
- Commander's Decision Making
- Staff's Information Process
- Coordination Requirements
- Communications Systems
- Computer Systems
- Intelligence Systems
- Other

Example

Disagree
Example

8. The next several questions relate to the disconnect between designers, testers and users of C4I systems. What are the main difficulties or issues in **designing** C4I systems from your experience?

Issue 1:

Issue 2:

Issue 3:

9. How do you explain these **design** difficulties? What causes these difficulties?

Cause(s) of Issue 1:

Cause(s) of Issue 2:

Cause(s) of Issue 3:

10. What is the effect or impact of these **design** difficulties on the testing or use of C4I systems? How do these issues manifest themselves in actual, operational C4I systems? Please cite a specific example to support your claim.

Effect(s) 1:

Effect(s) 2:

Effect(s) 3:

11. What ways can you suggest for mitigating these **design** difficulties or their causes and effects?

Suggestion 1:

Suggestion 2:

Suggestion 3:

12. What are the main difficulties or issues in **testing** C4I systems from your experience?

Issue 1:

Issue 2:

Issue 3:

13. How do you explain these **testing** difficulties? What causes these difficulties?

Cause(s) of Issue 1:

Cause(s) of Issue 2:

Cause(s) of Issue 3:

14. What is the effect or impact of these **testing** difficulties on the design or use of C4I systems? How do these issues manifest themselves in actual, operational C4I systems?

Effect 1:

Effect 2:

Effect 3:

15. What ways can you suggest for mitigating these **testing** difficulties or their causes and effects?

Suggestion 1:

Suggestion 2:

Suggestion 3:

16. What are the main difficulties or issues in **using** C4I systems from your experience?

Issue 1:

Issue 2:

Issue 3:

17. How do you explain these difficulties in **using** C4I systems? What causes these difficulties?

Cause(s) of Issue 1:

Cause(s) of Issue 2:

Cause(s) of Issue 3:

18. What is the effect or impact of these difficulties on the operation of C4I systems and their effectiveness in combat operations? How do these issues manifest themselves in actual, operational C4I systems?

Effect 1:

Effect 2:

Effect 3:

19. What ways can you suggest for mitigating these difficulties or their causes and effects?

Suggestion 1:

Suggestion 2:

Suggestion 3:

20. Now that you have thought about the difficulties in designing, testing, and using C4I systems and their causes and effects, how would you, in a summation, define the disconnect between designers, testers, and users of C4I systems?

Summary of Disconnect

21. Can you cite a specific example of a very successful C4I system or subsystem?

    Name of System

    Purpose of System

    Nature of System's Success

22. What were the main features or characteristics that made this system successful?

    Name of System

    Main Features

    Other

23. Can you cite a specific example of a problematic C4I system or subsystem?

    Name of System

    Main Problems

    Other

24. What were the main causes or characteristics that made this system problematic?

    Name of System

    Main Characteristics

    Other

25. Knowledge in systems engineering is often characterized as being of three types: practices, principles, and perspectives. What knowledge about C4I systems do you think is valuable in terms of standard practices, emerging principles, or promising future perspectives?

    Standard Practices

    Emerging Principles

    Promising Future Directions

26. Is there a question that I haven't asked that you think needs to be asked, what is it and how would you answer this question?

27. Who else should I talk to that could provide useful information on designing, testing, and using C4I systems?

28. Now that I have asked you questions without leading your answers, I would like to capture your thoughts on some focused issues relevant to C4I systems.

29. **Re-engineering** is a popular term which has come to mean examining business processes and operations in light of new technologies and current trends. In this sense, what impact will trends in information technology have on C2 processes and operations? How should **C2 processes** be re-engineered? (For instance, can you recommend any examples from business or industry that merit consideration?)

30. How would you **re-engineer the US. military** in light of information technology? **What changes in doctrine, force structure, operations, and training would you consider and why**? (Can you recommend any examples from business or industry that merit emulation?)

SOURCES CONSULTED

Andrews, Edmund L. "A Satellite System is Planned to Link Most of the Globe: Goal of Two Entrepreneurs, Craig McCaw and William Gates Propose to Spend $9 Billion on 840 Space Vehicles." *New York Times*, 21 March 1994.

Andriole, Stephen J., ed. *Advanced Technology for Command and Control Systems Engineering*. [Fairfax, Va.:]Armed Forces Communications and Electronics Association (AFCEA) International Press, 1990.

Anno, Stephen E. and William E. Einspahr. "Command and Control and Communications Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid." Air War College Research Report, No. AU-AWC-88-043, Air University, Maxwell Air Force Base, Ala.

Apple Computer Inc. *Macintosh Reference*. Cupertino, Ca.: Apple, 1989.

Apple, R. W., Jr. "Trigger Fingers: Has Technology Made Mishaps More Likely?" *New York Times*, 15 April 1994, 1.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!". *Comparative Strategy*. vol. 12, United Kingdom: Taylor & Francis, 1993, 141-65.

Arnett, Eric H. "Welcome to Hyperwar." *The Bulletin of the Atomic Scientists* 48, no. 1, (September 1992): 15.

Aspen Institute Forum. "Special Report: The Information Evolution: How New Information Technologies are Spurring Complex Patterns of Change." *Aspen Institute Forum*, 22 March 1993.

Atkinson, Rick. "The Raid That Went Wrong: How an Elite U.S. Force Failed in Somalia." *The Washington Post*, Sunday Final Edition, 30 January 1994, 1.

Bankes, Steve and Carl Builder. *Seizing the Moment: Harnessing the Information Technologies*. A RAND Note, RAND, Santa Monica, Ca: RAND, 1993.

Beam, Walter R. *Command, Control, and Communications Systems Engineering*. New York: McGraw-Hill, 1989.

Bloor, Robin. "Changing of the Guard: Moving to Client/Server Environments May Mean Updating Your Legacy Staff." *DBMS* 7, no. 4, (April 1994), 12.

Bodnar, John W. "The Military Technical Revolution from Hardware to Information." *Naval War College Review*. Summer 1993, 7-21.

Bracken, Paul. "The Military After Next." The Washington Quarterly. Autumn 1993, vol. 16, No. 4, pp. 157-174.

Budiansky, Stephen, Bruce B. Auster, Joseph L. Galloway, and Peter S. Green. "New Weapons of War." *U.S. News & World Report*, 31 May 1993, 30-33.

Buede, Dennis M., Didier M. Perdu, and Lee W. Wagenhals, "Modeling the Functionality of the C2 Element of the National Missile Defense System." In *Proceedings of the Symposium on Command and Control Research 28-29 June 1993*. Washington, D. C.: National Defense University Press, 1994, 246-255.

Canan, James W. "How to Command and Control a War." *Air Force Magazine*, April 1991.

Cassity, James S. Jr. "Command, Control Advances Permeate Combat Successes." *Signal Magazine*, May 1991.

Chairman of the Joint Chiefs of Staff. *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*. CJCS Instruction no. 6212.01, Washington, D.C.: U.S. Government Printing Office, 30 July 1993.

Coakley, Thomas P. *Command and Control for War and Peace*. With an Introduction by Robert T. Herres. Washington, D.C.: National Defense University Press, 1992.

Collinson, Peter. "Open Doors." *EXE*, February 1994, 36.

Cothier, Philippe H. and Alexander H. Levis. "Timeliness and Measures of Effectiveness in Command and Control." *IEEE Transactions on Systems, Man, and Cybernetics SMC-16*, no. 6, (November/December 1986), 844-51.

D. Appleton Company, Inc. *Corporate Information Management Process Improvement Methodology for DOD Functional Managers* 2. Fairfax, Va.: D. Appleton, 1993.

Defense Electronics, ed. *The C3I Handbook: Command Control Communications Intelligence 3*. Palo Alto, Calif.: EW Communications, Inc., 1988.

DePuy, William E. "Concepts of Operation: The Heart of Command, The Tool of Doctrine." Army Magazine, August 1988, 28.

Edmonds, Albert J. "C4I for the Warrior: Committed, Focused, and Needed." The Pentagon: C4 Architecture and Integration Division, J-6, The Joint Staff, 12 June 1993.

Endoso, Joyce. "Software Shops Won't Go to DISA: Paige Lets Central Design Activities Revert to the Services." *Government Computer News*, 19 July 1993, 1.

_____. "DOD Pushes for Standard Systems." *Government Computer News*, 27 September 1993, 1.

_____. "Pentagon Brass Behind Schedule in Nominating Standard Systems." *Government Computer News*, 7 February 1994, 3.

_____. "He's Off I-CASE Buy But Not the Program." *Government Computer News*, 7 March 1994, 14.

Freedman, Alan. *Electronic Computer Glossary*. The Computer Language Co. Inc., 1993.

Gibson, Timothy J. "Command, Control System Abets Victory in Gulf War." *Signal Magazine*, March 1992.

Gordon, Michael R. "26 Killed as U.S. Warplanes Down Two U.S. Helicopters Over Kurdish Area of Iraq." New York Times, 15 April 1994, 1.

Goure, Dan. "Is There a Military Technical Revolution in America's Future?" The Washington Quarterly, Autumn 1993, Vol. 16, No. 4, pp. 175.

Hall, Charles R., III. "An Approach to the Measurement of the Marginal Contribution of C4I Enhancements to Force Effectiveness." working paper, Naval Systems and Technology Division, MITRE Corporation, 5 May 1994.

Kador, John. "One on One." *Midrange Systems*, 11 February 1994, 46.

Laurel, Brenda. "Anatomy of a Fad: Post-Virtual Reality, after the Hype Is Over." *Digital Media* 2, no.10-11 (29 March 1993): 2-7.

Lindsay, Don. "The Limits of Chip Technology." *Microprocessor Report*, 25 January 1993, 21.

Levine, Ron. "Look, Ma, No Wires!: How Digital Wireless Communications Technology is Changing the Field Service Frontier." *DEC Professional*, 12 no.5 (May 1993): 64.

Macke, R. C., "Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems," an unclassified staff instruction signed by the Director, Joint Staff for the Chairman, Chairman of the Joint Chiefs of Staff Instruction 6212.01, 30 July 1993.

Miller, Michael J. "The Myth of Usability." *PC Magazine*, 12 April 1994, 79-80.

Minton, Carol. "War Stories on the Software Testing Front." *Midrange Systems*, 11 February 1994, 28.

National Security Industrial Association. *Army Command, Control, Communications, and Automation*. NSIA: September 1993.

Newton, Harry. *Newton's Telecomm Dictionary*. Harry Newton, 1994.

O'Berry, Carl G. *Horizon: Air Force C4I Strategy for the 21st Century*. The Pentagon: U.S. Air Force Deputy Chief of Staff for Command, Control, Communications, and Computers, no date on document.

Oxley, Ron. "Defense Management Report Decision 918 Fact Sheet." Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, 17 February 1993.

Paige, Emmett Jr. "Re-Engineering DoD's C3I Operations." *Defense 93*, Issue 6, Washington, D.C.: U.S. Government Printing Office, 1993, 15-22.

Parker, Rachel. "Better Access, Development Time Sell Client/Server." *InfoWorld*, 18 April 1994, 74.

Perry, William J. "Three Barriers to Major Defense Acquisition Reform." *Defense 94*, Issue 1, Washington, D.C.: U.S. Government Printing Office, 2-5.

Piraino, John K. "Preparing for the 21st Century: Client/Server More Than a Technology, It is a Management Philosophy." *DBMS* 6, no. 13, (December 1993), 10.

Prosise, Jeff. "Under Construction: Plug and Play." *PC Magazine*, 12 April 1994, 204.

Rechter, R. J. et al., "Army Tactical Command and Control Systems: An Integrated Approach," in *Advanced Technology for Command and Control Systems Engineering*, ed. Stephen J. Andriole, 439-451, Fairfax, Va.: AFCEA International Press, November 1990.

Ricke, Thomas E. "U.S. Fighters Accidentally Shoot Down Two American Helicopters Over Iraq." *Wall Street Journal*, 15 April 1994, 10.

Sage, Andrew P. *Systems Engineering*. New York: John Wiley, 1992.

Schwarzkopf, Norman H. with Peter Petre. *It Doesn't Take a Hero*. New York: Bantam, 1992.

Shoffner, D. "Future Battlefield Dynamics and Complexities Require Timely and Relevant Information." *PHALANX*, (March 1993): 1.

Slim, William. "Higher Command in War." Kermit Roosevelt lecture, US Army Command and General Staff College, Fort Leavenworth, Kansas, date, p. 8.

Snyder, Frank M. *Command and Control: The Literature and Commentaries*. Washington, D.C.: National Defense University Press, 1993.

Sovereign, Michael, W. Kemple, and J. Metzger. "C3IEW Measures Workshop II." *PHALANX* 27, no. 1, (March 1994), 10-14.

Strassman, Paul. "Letter to the Editor." *Government Computer News*, 16 August 1993, 30.

Sullivan, Gordon R. and John W. Shannon. *Strategic Force- Decisive Victory: A Statement on the Posture of The United States Army Fiscal Year 1994*, Washington, D.C.: U.S. Government Printing Office, March 1993.

Sun Tzu. *The Art of War*. Edited by James Clavell. New York: Delacorte Press, 1983.

Tuttle, Jerry O. "Sonata," an unclassified pamphlet signed by the Director, Navy C2 Systems, September 1993.

U.S. Department of the Army. *Army Enterprise Strategy: Vision*. Director of Information Systems for Command, Control, Communications, and Computers, Washington, D.C.: U.S. Government Printing Office, 20 July 1993.

U.S. Department of the Army. *Field Manual 100-5, Operations*. Washington, D.C.: U.S. Government Printing Office, 14 June 1993.

U.S. Defense Information Systems Agency. *Department of Defense Technical Architecture Framework for Information Management*. Coordination Draft, Vol. 2, *Technical Reference Model and Standards Profile*, Version 2.0. Washington, D.C.: U.S. Government Printing Office, 22 June 1993.

U.S. Department of Defense. Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence Systems. DOD Directive no. 4630.5, Washington, D.C.: U.S. Government Printing Office, 12 November 1992.

U.S. Department of Defense. *Conduct of the Persian Gulf War: Final Report to Congress*. Washington, D.C.: U.S. Government Printing Office, 1992.

U.S. Department of Defense. *Report of the Defense Science Board Task Force on Defense Acquisition Reform*. Washington, D.C.: U.S. Government Printing Office, July 1993.

U.S. Department of Defense. *Technical Reference Model for Information Management.* Version 1.3, Defense Information Systems Agency Center for Information Management, Washington D. C.: U.S. Government Printing Office, 31 December 1992.

U.S. General Accounting Office. *Army Battlefield Automation: Oversight.* Washington D.C.: U.S. Government Printing Office, 1990.

U.S. General Accounting Office. *Test and Evaluation: DOD Has Been Slow In Improving Testing of Software-Intensive Systems.* no. NSIAD-93-198, Washington, D.C.: U.S. Governement Printing Office, 29 September 1993.

U.S. General Accounting Office. *Software Reuse: Major Issues Need to be Resolved Before Benefits Can Be Achieved.*. no. IMTEC-93-16, Washington, D.C.: U.S. Governement Printing Office, 28 January 1993.

Von Clausewitz, Carl. Edited and translated by Michael Howard and Peter Paret. *On War.* Princeton: Princeton University Press, 1976.

Winsburg, Paul. "What About Legacy Systems?" Database Programming and Design 7, no. 3, (March 1994): 23.

Woodward, Sandy. *One Hundred Days: The Memoirs of the Falklands Battle Group Commander.* Annapolis: Naval Institute Press, 1992.

Zepezauer, Steven V. "Racing Into the Interactive Age." *Graduating Engineer*, January 1994, 24.

INTERVIEWS

Barron, Mike, Army Signal Corps Officer, Chief, Architecture and Integration Branch, Joint Staff J-6 Integration Division, The Pentagon. Interview by author, 6 April 1994, Arlington. The Pentagon, Arlington, Va.

Bean, Theodore T., Special Assistant for Tactical Command and Control, Battlefield Systems Division, MITRE Corp. Interview by author, 3 May 1994, Washington. MITRE Corporation, Reston, Va.

Bossio, Frank Naval Staff Officer, OPNAV N6C, Command, Control, Communications, and Computers, Navy Staff, The Pentagon. Interview by author, 17 May 1994. Naval War College, Newport, Rhode Island.

Buede, Dennis, Associate Professor and Researcher, Center for Excellence in Command, Control, Communications, and Intelligence, School of Information Technology and Engineering, George Mason University. Interview by author, 7 April 1994, Washington. Written notes. George Mason University, Fairfax, Va.

Cebrowski, Arthur K., Vice Admiral, U.S. Navy, Director of Space and Electronic Warfare, Department of the Navy. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Clouser, Dan, Analyst and Department Head, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corporation, Reston, Va.

Curtis, Keith, Analyst and Group Leader, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corporation, Reston, Va.

Edmonds, Albert J., Lieutenant General, U.S. Air Force, Director Command, Control, Communications, and Computer Systems, The Joint Staff. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Federici, Gary, Director for Communications, Space, and Electronic Systems Program, Center for Naval Analyses. Interview by author, 2 May 1994, Alexandria. Written notes. Center for Naval Analyses, Alexandria, Va.

Freck, Peter G., Director of Army Programs, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corporation, Reston, Va.

Gray, Robert E., Major General, U.S. Army, Commanding General, U.S. Army Signal Center and School. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Hall, Charles R., III, Director Naval Systems and Technology Office, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corporation, Reston, Va.

Holmes, Justin A. Associate Department Head, Washington C3 Center, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corporation, Reston, Va.

Kind, Peter A., Lieutenant General, U.S. Army, Director of Information Systems for Command, Control, Communications, and Computers, Office of the Secretary of the Army. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Long, Scott, Army Signal Corps Officer, Office of the Director of Information Systems for Command, Control, Communications, and Computers, Office of the Secretary of the Army. Interview by author, 4 May 1994, The Pentagon. Written notes. The Pentagon, Arlington, Va.

Miller, Hap, Senior Analyst, Institute for Defense Analysis. Interview by author, 5 May 1994, West Point. Written notes. Operations Research Center, United States Military Academy, West Point, New York.

Minihan, Kenneth A., Major General, U.S. Air Force, Director Joint Electronic Warfare Center. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

O'Brasky, James S., Chief Analyst, Warfare Analysis Department, Naval Surface Warfare Center. Interview by author, 17 May 1994, Newport. Written notes. Naval War College, Newport, Rhode Island.

O'Brien, Peter A., Naval War College Student and Former Naval Intelligence Officer for Chief US Military Training Mission Rhiyadh Saudi Arabia and Former Intelligence Officer for US Central Command Planning Cell J-5 Forward, Former Naval Wing Intelligence Officer. Interview by author, 25 May 1994, Newport. Written notes. Naval War College, Newport, Rhode Island.

Oden, Leonard N., Rear Admiral, U.S. Navy, Deputy Director Space and Electronic Warfare, Department of the Navy. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Pullen, Martin, Professor and Researcher, Center for Excellence in Command, Control, Communications, and Intelligence, School of Information Technology and Engineering, George Mason University. Interview by author, 7 April 1994, Fairfax. Written notes. Fairfax, Va.

Signori, David T. Jr., Deputy Director Designee, Defense Information Systems Agency. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Snyder, Frank M., Professor Emeritus of Military Command and Control, Naval War College. Interview by author, 26 April 1994, Newport. Written notes. Naval War College, Newport, Rhode Island.

Starr, Stuart, Senior Director, MITRE Corp. Interview by author, 5 April 1994, Reston. Written notes. MITRE Corp., Reston, Va.

Van Riper, Paul K., Major General, U.S. Marine Corps, Assistant Chief of Staff Command, Control, Communications, and Computers and Intelligence, Headquarters, U.S. Marine Corps. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Wagenhals, Lee W., C3I Analyst and Researcher. Interview by author, 6 April 1994, Fairfax. Written notes. Center for Excellence in C3I, School of Information Technology and Engineering, George Mason University, Fairfax, Va.

Witt, Buford R., Brigadier General, U.S. Air Force, Director Plans, Policy, and Resources, Office of the Deputy Chief of Staff for Command, Control, Communications, and Computers, The Air Staff. Remarks from address to the Information-Based Warfare Symposium, 3 May 1994, Washington. Written notes. National Defense University, Washington, D.C.

Zaj, Bruce, Army Signal Corps Officer, Office of the Director of Information Systems for Command, Control, Communications, and Computers. Interview by author, 13 April 1994, The Pentagon. Written notes. The Pentagon, Arlington, Virginia.